

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA :

Plaintiff, :

v.

20 Cr. 015 (PKC)

:

VIRGIL GRIFFITH,

:

Defendant.

-----X

**APPENDIX OF EXHIBITS IN SUPPORT OF DEFENDANT'S
MOTIONS FOR A BILL OF PARTICULARS, TO DISMISS,
AND TO COMPEL**

BRIAN E. KLEIN
KERI CURTIS AXEL
BAKER MARQUART LLP
777 S. Figueroa Street, Suite 2850
Los Angeles, California 90017
(424) 652-7800

SEAN S. BUCKLEY
KOBRE & KIM LLP
800 Third Avenue
New York, New York 10022
(212) 488-1200

Attorneys for Virgil Griffith

Defendant Virgil Griffith respectfully submits the following exhibits in support of his Motion for a Bill of Particulars, Motion To Dismiss, and Motion to Compel:

1. Attached as Exhibit A is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001746 to USAO_001747.....pages 4-6
2. Attached as Exhibit B is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001754.....pages 7-8
3. Attached as Exhibit C is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001752.....pages 9-10
4. Attached as Exhibit D is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001755 to USAO_001759.....pages 11-16
5. Attached as Exhibit E is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001745.....pages 17-18
6. Attached as Exhibit F is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001744.....pages 19-20
7. Attached as Exhibit G is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_006900 to USAO_006901.....pages 21-23
8. Attached as Exhibit H is a true and correct copy of the document produced by the government in this matter Bates stamped USAO_001751.....pages 24-25
9. Attached as Exhibit I is a true and correct copy of the indictment in the case *United States v. Attila*, Case No. 15 Cr. 867 (RMB).....pages 26-79
10. Attached as Exhibit J is a true and correct copy of the indictment in the case *United States v. Nejad*, Case No. 18 Cr. 224 (AJN).....pages 80-114
11. Attached as Exhibit K is a true and correct copy of the indictment in the case *United States v. Banki*, Case No. 10 Cr. 08 (JFK).....pages 115-137
12. Attached as Exhibit L is a true and correct copy of the indictment in the case *United States v. Huawei Techs. et al.*, Case No. 1:18-cr-00457-AMD.....pages 138-194

13. Attached as Exhibit M is a true and correct copy of the indictment in the case *United States v. Dandong Hongxiang Indus. Dev. Co. Ltd., et al*, Case No. 2016-mj-06602...pages 195-219

Dated: January 12, 2021

Respectfully Submitted,

/s/ Brian E. Klein

Brian E. Klein

Keri Curtis Axel

Baker Marquart LLP

-and-

Sean S. Buckley

Kobre & Kim LLP

Attorneys for Virgil Griffith

EXHIBIT A

From: [McKenzie, Matthew \(NSD\)](#)
To: [\[REDACTED\]@treasury.gov](#)
Cc: [\[REDACTED\] \(NSD\)](#); [Ravener, Kimberly \(USANYS\)](#); [Krouse, Michael \(USANYS\)](#); [Wirshba, Kyle \(USANYS\)](#)
Subject: Request for Expedited OFAC License Determination
Date: Tuesday, November 19, 2019 9:31:00 AM
Attachments: [v8 Griffith Complaint \(to OFAC\).pdf](#)

Good morning [REDACTED]

CES and SDNY are requesting an OFAC Licensing Determination in the matter of Virgil Griffith (Griffith). Please find below an outline of the relevant facts and arguments along with the attached draft criminal complaint. If you have any questions or require additional information, please do not hesitate to call me at [REDACTED]. Please note that the FBI considers Griffith to be a flight risk. As a result, we ask that OFAC make a licensing determination as soon as possible to enable the FBI to effect an arrest this week.

-
Background

Griffith is a United States citizen living in Singapore who possesses advanced technical degrees and currently works for the Swiss based cryptocurrency company Ethereum Foundation, an open-source platform for the development of blockchain and cryptocurrency technologies, including, among other things, the cryptocurrency Ethereum. In April 2019, Griffith traveled to the DPRK to attend and present at the "Pyongyang Blockchain and Cryptocurrency Conference." According to Griffith, his presentation was titled "Blockchain and Peace."

Relevant Facts

In three interviews with the FBI, Griffith described the conference, the development of his presentation, and his presentation to conference participants. In particular, Griffith stated that before he developed his presentation, the organizers of the conference researched general blockchain and cryptocurrency PDFs on the internet and provided them to the DPRK, seeking permission to discuss the PDFs' content at the conference. Upon receiving DPRK approval, the organizers provided the PDFs to Griffith prior to his travel and Griffith developed a PowerPoint presentation based on the PDFs' topics. During the conference, one of the conference's organizers told Griffith that his presentation should include cryptocurrency and blockchain concepts that could be used for money laundering and sanctions evasion. The organizer stressed that Griffith should use the phrase "money laundering" in his presentation as it resonated with the DPRK audience.

Griffith further described that, at his presentation, the display computer had technical problems so Griffith discussed the topics verbally with attendees and utilized a whiteboard to draw diagrams illustrating his lecture. According to Griffith, the presentation covered, among other topics, establishing a blockchain "smart contract" to avoid the United Nations "court system," and how "smart contracts" might allow the DPRK government to contract with a media outlet to ensure the outlet publishes only approved content. In describing his presentation to the FBI, Griffith agreed with agents that the PDFs that the organizers provided were like a course textbook and Griffith acted as the lecturer who explained the content to the audience like a teacher.

Griffith also noted that, at his presentation, there were approximately three young males that asked more technical and specific questions. These included questions about the “dark web” and cryptocurrency topics such as “proof of work” versus “proof of stake,” concepts concerning the creation of certain cryptocurrencies such as Ethereum in a process known as “mining.”

In addition, Griffith’s cellphone—extracted on consent—confirmed that before the conference, Griffith understood that the DRPK’s interest in cryptocurrency was “probably sanctions evasion . . . who knows.” Indeed, even after the conference and his initial interview with FBI, Griffith has continued to talk about going back to the DPRK and has tried to convince at least two other US citizens to do so.

Relevant Law

The IEEPA excludes from its licensing requirements “the . . . exportation to any country . . . of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.” 50 U.S.C. § 1702(b)(3). Attendant regulations clarify that this exception does not include “materials not fully created and in existence at the date of the transactions, or to the substantive or artistic alteration or enhancement of informational materials” 31 C.F.R. § 560.210.

Analysis

Griffith’s presentation does not fall under the material or information materials exception because Griffith created the presentation for the cryptocurrency conference and the DPRK government. In his presentation, Griffith lectured on using smart contracts to avoid the UN “court system” and make binding agreements with media entities looking to enter the DPRK. These topics are only relevant to a sanctioned government like the DPRK and are inapposite to any general presentation on blockchain or cryptocurrency technology. In addition, Griffith took questions during which, by his own admission, Griffith discussed with more knowledgeable conference attendees topics such as the creation of cryptocurrency through mining.

That the basis for Griffith’s presentation was publically available information does not undermine this conclusion. Griffith used his expertise to take publically available information and package it so that the DPRK audience could better understand the concepts and apply it to circumstances that were unique to issues present in particular within the DPRK. Doing so is providing a service to the DPRK beyond the mere provision of information materials. Griffith’s conduct stands in stark contrast with someone providing newspapers. Here, Griffith’s conduct is more analogous to someone interpreting the news for the DPRK government to assist them in their foreign policy considerations—surely a violation of IEEPA.

Matthew J. McKenzie

Trial Attorney

Counterintelligence and Export Control Section

EXHIBIT B

Protected Material

From: [REDACTED]
To: [REDACTED]; McKenzie, Matthew (NSD); Wirshba, Kyle (USANYS)
Cc: [REDACTED]; Ravener, Kimberly (USANYS); Krouse, Michael (USANYS)
Subject: RE: Request for Expedited OFAC License Determination
Date: Wednesday, November 20, 2019 5:09:52 PM

PRIVILEGED/DELIBERATIVE/PRE-DECISIONAL

All, for your awareness:

[REDACTED] and I just spoke with OFAC. I expect we'll be able to get back to you tomorrow (hopefully by noon) with the assurance you need, at least as to Griffith's presentation at the conference. On the facts presented, OFAC may not be comfortable giving the assurance with respect to Griffith's travel to NK.

If you have questions in the meantime, feel free to call or email me or [REDACTED]. Thanks.

[REDACTED]

From: [REDACTED]
Sent: Wednesday, November 20, 2019 1:00 PM
To: 'McKenzie, Matthew (NSD)'; [REDACTED]; Wirshba, Kyle (USANYS)
Cc: [REDACTED]; Ravener, Kimberly (USANYS)
[REDACTED]; Krouse, Michael (USANYS); [REDACTED]; [REDACTED]
Subject: RE: Request for Expedited OFAC License Determination

Thanks, that works for Treasury.

[REDACTED]

[REDACTED]
Attorney-Advisor
Office of the Chief Counsel (Foreign Assets Control)
U.S. Department of the Treasury
Office [REDACTED]
Cell: [REDACTED]

From: McKenzie, Matthew (NSD); [REDACTED]
Sent: Wednesday, November 20, 2019 12:56 PM
To: Wirshba, Kyle (USANYS); [REDACTED]
Cc: [REDACTED]; [REDACTED] (NSD)
[REDACTED]; Ravener, Kimberly (USANYS); [REDACTED]
Krouse, Michael (USANYS); [REDACTED]
Subject: RE: Request for Expedited OFAC License Determination

EXHIBIT C

From: [REDACTED]
To: [Wirshba, Kyle \(USANYS\)](#); [McKenzie, Matthew \(NSD\)](#)
Cc: [REDACTED]; [Ravener, Kimberly \(USANYS\)](#); [Krouse, Michael \(USANYS\)](#); [REDACTED]
Subject: DPRK sanctions case
Date: Thursday, November 21, 2019 1:32:57 PM
Attachments: [v8 Griffith Complaint \(to OFAC\).pdf](#)
[2019.11.15 SA Cavanaugh License History Check.pdf](#)

PRIVILEGED/DELIBERATIVE/PRE-DECISIONAL

This confirms that if asked, OFAC will provide a witness to testify that the facts set out in the attached Sealed Complaint show violations of the North Korea Sanctions Regulations, 31 CFR Part 510. The witness would testify that the presentation by Virgil Griffith at the Cryptocurrency Conference in North Korea referenced in the Sealed Complaint constituted a violation of 31 CFR §§ 510.206(a) (prohibited exportation of services to North Korea) and 510.212(b) (conspiracy to violate prohibitions set forth in 31 CFR Part 510).

The witness would also testify that on November 15, 2019, OFAC conducted a License History Check to determine whether its records indicate that Mr. Griffith ever sought or obtained a license from OFAC to participate in the Cryptocurrency Conference. The witness would testify that the search disclosed no responsive records of applications submitted by or on behalf of, and no OFAC licenses issued to, any party by the name of Virgil Griffith. See the attached License History Check.

Please feel free to contact me or [REDACTED] if you have questions.

[REDACTED]

[REDACTED]

Chief Counsel, Office of Foreign Assets Control

[REDACTED]

[REDACTED]

EXHIBIT D

Protected Material

From: [Cavanaugh, Brandon M. \(NY\) \(FBI\)](#)
To: [REDACTED]
Subject: RE: RE: FW: 302 and Griffith Update
Date: Wednesday, November 20, 2019 11:55:00 AM

Thanks!

Brandon Cavanaugh
SA / FBI New York
[REDACTED]
[REDACTED]

From: [REDACTED]
Sent: Wednesday, November 20, 2019 11:47 AM
To: [REDACTED] (IP) (FBI) [REDACTED] Cavanaugh, Brandon M. (NY) (FBI)
[REDACTED]; [REDACTED] (NY) (FBI) [REDACTED]; [REDACTED] (CD)
(FBI) [REDACTED] >
Subject: RE: RE: FW: 302 and Griffith Update

Hi Brandon,

[REDACTED] is the AD of OFAC Enforcement. He is the one we can coordinate with if necessary. Usually we would simply submit the fact pattern for a License Determination to the Enforcement hotline, but if we are seeking quick turnaround we can engage with [REDACTED] directly, as his team would handle the response. [REDACTED] contact info is below:

[REDACTED]
[REDACTED]

I've got a good relationship with [REDACTED] and his Chiefs, let me know if you want me to engage them.
Thanks,
[REDACTED]

From: [REDACTED] (IP) (FBI) [REDACTED]
Sent: Wednesday, November 20, 2019 11:35 AM
To: [REDACTED]
Subject: Fwd: RE: FW: 302 and Griffith Update

-

----- Forwarded message -----

From: "Cavanaugh, Brandon M. (NY) (FBI)" [REDACTED]
 Date: Nov 20, 2019 11:09 AM
 Subject: RE: FW: 302 and Griffith Update
 To: [REDACTED] (CD) (FBI)" [REDACTED] (IP) (FBI)"
 <[REDACTED] (NY) (FBI)" [REDACTED]>
 Cc:

Thanks all. There appears to be a DOJ/OFAC call at 2pm. But we don't want to hit anyone up on it since the situation is sensitive. For my AUSA's awareness, what is the name of the OFAC Enforcement section chief? He may reference this OFAC license determination suggestion in the call.

 Brandon Cavanaugh
 SA / FBI New York
 [REDACTED]
 [REDACTED]

From: [REDACTED] (CD) (FBI)
Sent: Tuesday, November 19, 2019 5:45 PM
To: Cavanaugh, Brandon M. (NY) (FBI) [REDACTED]; [REDACTED] (IP) (FBI)
 [REDACTED]; [REDACTED] (NY) (FBI) <[REDACTED]>
Subject: RE: FW: 302 and Griffith Update

Thanks [REDACTED]. I defer to New York to determine when to submit this. Have a good night.

-

On Nov 19, 2019 5:32 PM, [REDACTED] (IP) (FBI)" [REDACTED] wrote:
 Sounds good. If they are not getting what they need from OFAC counsel, let me know. It sounds to me they may need a license determination from OFAC enforcement.

Its just the facts of the case, and OFAC determines if a licenses is required for that activity. If so, and one was not obtained, it's a violation.

It is submitted to OFACs Law Enforcment hotline: [REDACTED]

Please reach out if you want to do this, and I'll flag it for the appropriate Section Chief in OFAC Enforcement.

Thanks,
 [REDACTED]

-

On Nov 19, 2019 4:45 PM, [REDACTED] (CD) (FBI)" [REDACTED] wrote:
 Adam,

I spoke with Brandon in NY. He is going to talk with their SDNY AUSA. If they feel it prudent, the

AUSA will recommend to CES to contact OFAC Enforcement. Do you have a name of someone in enforcement as a POC?

Thanks,

From: Cavanaugh, Brandon M. (NY) (FBI)

Sent: Monday, November 18, 2019 8:07 PM

To: [REDACTED] (CD) (FBI); [REDACTED] (NY) (FBI) [REDACTED] >

Subject: Fwd: FW: 302 and Griffith Update

Hey sir. Its [REDACTED] However, DOJ asked us to hang on reaching out to OFAC. Apparently, one or more people have already reached out to [REDACTED] and he's becoming frustrated. Just wanted you to be aware of the sensitivity. Im free to chat on my cell if you need more tonight.

Brandon Cavanaugh
SA / FBI New York
[REDACTED]

On Nov 18, 2019 7:39 PM, [REDACTED] (CD) (FBI)" [REDACTED] wrote:
Good evening guys, do you have the name of the OFAC attorney?

-

----- Forwarded message -----

From: "[REDACTED] (IP) (FBI)" [REDACTED]

Date: Nov 18, 2019 5:30 PM

Subject: FW: 302 and Griffith Update

To: [REDACTED] (CD) (FBI)" [REDACTED]

Cc: [REDACTED] (CD) (FBI)" [REDACTED] >

Sure. Do you know the OFAC attorney they consulted with?

I imagine the issue at hand is the activity itself and what constitutes a service. I can speak with them.

-

On Nov 18, 2019 5:03 PM, [REDACTED] (CD) (FBI)" [REDACTED] > wrote:
Adam,

I am tracking a case out of NY where they have identified an USPER who, after seeking and being denied permission by DoS, voluntarily traveled to the DPRK to attend a cryptocurrency symposium. The purpose was to assist the DPRK in creating their own cryptocurrency platform. New York interviewed him twice and he admitted going. SDNY is working to obtain a complaint so we can

effect an arrest on an IEEPA charge. It looks as if CES has consulted with OFAC (I imagine this is customary in IEEPA cases?) and the OFAC attorney is having concerns. Is there anything we can do to provide additional information to OFAC to assist in articulating the fact pattern? Please let me know.

Thanks,

[REDACTED]

From: [REDACTED] (NY) (FBI)
Sent: Monday, November 18, 2019 4:55 PM
To: [REDACTED] (CD) (FBI) [REDACTED]
Cc: Cavanaugh, Brandon M. (NY) (FBI) [REDACTED]
Subject: FW: 302 and Griffith Update

From: Cavanaugh, Brandon M. (NY) (FBI)
Sent: Monday, November 18, 2019 3:30 PM
To: [REDACTED] (NY) (FBI) [REDACTED]
Subject: FW: 302 and Griffith Update

 Brandon Cavanaugh
 SA / FBI New York

[REDACTED]
 [REDACTED]

From: Wirshba, Kyle (USANYS) [REDACTED]
Sent: Monday, November 18, 2019 1:04 PM
To: Cavanaugh, Brandon M. (NY) (FBI) [REDACTED]
Subject: Fwd: 302 and Griffith Update

Kyle A. Wirshba
 Assistant United States Attorney
 United States Attorney's Office
 Southern District of New York
 One Saint Andrew's Plaza
 New York, NY 10007
 [REDACTED]

Begin forwarded message:

From: "McKenzie, Matthew (NSD)" [REDACTED]
Date: November 18, 2019 at 1:01:27 PM EST
To: "Wirshba, Kyle (USANY)" <[REDACTED]>
Subject: RE: 302 and Griffith Update

Do we know how much of the presentation he gave was specifically created for this event vs. a general presentation that he gives otherwise. OFAC says that this is a grey area and general presentations that are given other places may fall under an exception and not require a license, while a specifically created presentation would be a service.

I am going back through the 302s now to where it talks about how the DPRK screened it.

Matthew J. McKenzie

Trial Attorney
Counterintelligence and Export Control Section
U.S. Department of Justice
National Security Division

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

EXHIBIT E

Protected Material

From: [McKenzie, Matthew \(NSD\)](#)
To: [Wirshba, Kyle \(USANYS\)](#)
Subject: RE: 302 and Griffith Update
Date: Monday, November 18, 2019 1:01:30 PM

Do we know how much of the presentation he gave was specifically created for this event vs. a general presentation that he gives otherwise. OFAC says that this is a grey area and general presentations that are given other places may fall under an exception and not require a license, while a specifically created presentation would be a service.

I am going back through the 302s now to where it talks about how the DPRK screened it.

Matthew J. McKenzie

Trial Attorney
 Counterintelligence and Export Control Section
 U.S. Department of Justice
 National Security Division

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

From: Wirshba, Kyle (USANYS) [REDACTED]
Sent: Monday, November 18, 2019 12:59 PM
To: McKenzie, Matthew (NSD) [REDACTED] >
Subject: Re: 302 and Griffith Update

If you don't get me try my cell at [REDACTED]

Any preview?

Kyle A. Wirshba
 Assistant United States Attorney
 United States Attorney's Office
 Southern District of New York
 One Saint Andrew's Plaza
 New York, NY 10007

[REDACTED]

On Nov 18, 2019, at 12:57 PM, McKenzie, Matthew (NSD) <[REDACTED]>
 wrote:

Kyle,

Sorry, I was on the other line. I just walked down to [REDACTED]'s office and she is speaking to someone. We will call as soon as she is done.

EXHIBIT F

From: [Krouse, Michael \(USANYS\)](#)
To: [Wirshba, Kyle \(USANYS\)](#)
Subject: RE: Griffith
Date: Monday, November 18, 2019 1:45:44 PM

I'm available from now to 3pm, and then again after 4pm (I think)—I have a bail hearing at 3.

We should probably tell the chiefs.

From: Wirshba, Kyle (USANYS) [REDACTED]
Sent: Monday, November 18, 2019 1:42 PM
To: Krouse, Michael (USANYS) [REDACTED] >
Subject: Griffith

So of course the deputy chief has problems. She talked to OFAC (who will have to be a witness on licensing) who are concerned that Griffith's presentation falls into the exception for "information or informational materials," 50 USC 1702(b)(3).

They are trying to set up a call with OFAC this afternoon. Do you have availability? Do we need to post the chiefs?

I'll put together everything we know about the presentation.

Kyle A. Wirshba
Assistant United States Attorney
United States Attorney's Office
Southern District of New York
One Saint Andrew's Plaza
New York, NY 10007
[REDACTED]

EXHIBIT G



FEDERAL BUREAU OF INVESTIGATION
Liaison with an Organization Outside of the FBI

Title: [REDACTED] Teleconference with Department of
Treasury

Date: 10/24/2019

Approved By: SSA [REDACTED]

Drafted By: CAVANAUGH BRANDON MICHAEL

Case ID #: [REDACTED] (U//FOUO) KoryoCoin/TokenKey, [REDACTED]
[REDACTED]/Virgil Griffith

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Responsible Organization: NEW YORK

Liaison Details: [REDACTED] Teleconference with Department of Treasury regarding subjects of captioned case. Treasury participants included [REDACTED] (Office: [REDACTED], NSTS: [REDACTED], JWICS:

[REDACTED], SIPRNET: [REDACTED]

Unclassified: [REDACTED] in Cyber Analysis Office, Office of Intelligence and Analysis, and [REDACTED] (Office: [REDACTED]

[REDACTED] NSTS: [REDACTED] JWICS: [REDACTED], in North Korea section, Office of Global Targeting, Office of Foreign Assets Control.

Writer and Treasury discussed de-conflicting equities related to captioned case. FBI advised of likely outcomes and ongoing investigative methods. Both shared recent intelligence reporting and identified remaining key intelligence questions. FBI and Treasury will continue to coordinate to enable intelligence collection of sources with access to captioned case and prior to enforcement actions such as OFAC designations and/or criminal charges. Treasury confirmed reporting of a second annual Pyongyang Blockchain and Cryptocurrency in 2020 and possible deterrence measures in advance to mitigate threats to national security.

[REDACTED]

[REDACTED]
Title: [REDACTED] Teleconference with Department of Treasury
Re: [REDACTED] 10/24/2019

Additionally, possible indictment of co-conspirators and/or US citizens as a deterrent to prospective attendees to the upcoming conference who may be exposed to criminal/legal risk.

Liaison Event: Meeting

Event Role: Conducted

Audience Type: None specified

Initiative Type: None specified

Total Attendees: 3

◆◆

EXHIBIT H

From: [Krouse, Michael \(USANYS\)](#)
To: [REDACTED]
Cc: [Wirshba, Kyle \(USANYS\)](#); [Ravener, Kimberly \(USANYS\)](#)
Subject: Call with OFAC
Date: Wednesday, November 20, 2019 2:24:25 PM

It went well. Thanks to Kyle's advocacy, the OFAC people said they would get us an answer promptly, and signaled that they would support the prosecution.

This is the lawyer Griffith said he retained:

[REDACTED]

EXHIBIT I

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA

- v. -

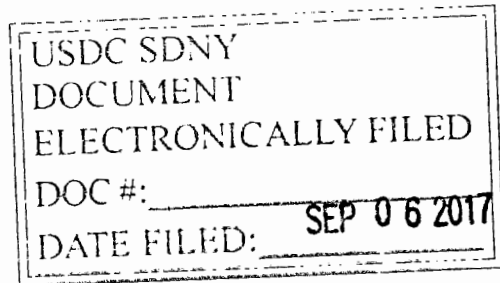
REZA ZARRAB,
a/k/a "Riza Sarraf,"
MEHMET HAKAN ATILLA,
MEHMET ZAFER CAGLAYAN,
a/k/a "Abi,"
SULEYMAN ASLAN,
LEVENT BALKAN,
ABDULLAH HAPANI,
MOHAMMAD ZARRAB,
a/k/a "Can Sarraf,"
a/k/a "Kartalmsd,"
CAMELIA JAMSHIDY,
a/k/a "Kamelia Jamshidy," and
HOSSEIN NAJAFZADEH,

Defendants.

- - - - - x

SUPERSEDING INDICTMENT

S4 15 Cr. 867 (RMB)



BACKGROUND

1. The charges in this indictment arise out of a multi-year scheme to violate and evade U.S. national security controls against the Government of Iran. In particular, money service businesses and front companies in Iran, Turkey, the United Arab Emirates, and elsewhere were used to violate and evade prohibitions against Iran's access to the U.S. financial system and restrictions on the use of proceeds of Iranian oil and gas sales and on the supply of gold to the Government of Iran and Iranian entities and persons.

2. High-ranking government officials in Iran and Turkey participated in and protected this scheme. Some officials received bribes worth tens of millions of dollars paid from the proceeds of the scheme so that they would promote the scheme, protect the participants, and help to shield the scheme from the scrutiny of U.S. regulators.

3. The leaders of a Turkish bank majority-owned by the Government of Turkey ("Turkish Bank-1") knowingly facilitated the scheme, participated in the design of fraudulent transactions intended to deceive U.S. regulators and foreign banks, and lied to U.S. regulators about Turkish Bank-1's involvement.

4. The proceeds of Iran's sale of oil and gas to Turkey's national oil company and gas company, among others, were deposited at Turkish Bank-1, in accounts in the names of the Central Bank of Iran, the National Iranian Oil Company ("NIOC"), and the National Iranian Gas Company. Because of U.S. sanctions against Iran and the anti-money laundering policies of U.S. banks, it was difficult for Iran to access these funds in order to transfer them back to Iran or to use them for international financial transfers for the benefit of Iranian government agencies, banks, and businesses.

5. Turkish Bank-1 participated in several types of transactions for the benefit of Iran that, if discovered, exposed Turkish Bank-1 to sanctions under U.S. law, including: (1) allowing the proceeds of sales of Iranian oil and gas deposited at Turkish Bank-1 to be used to buy Turkish gold that was not exported to Iran, in violation of the so-called "bilateral trade" rule; (2) allowing the proceeds of sales of Iranian oil and gas deposited at Turkish Bank-1 to be used to buy gold for the benefit of the Government of Iran; and (3) facilitating transactions fraudulently designed to appear to be purchases of food and medicine by Iranian customers, in order to appear to fall within the so-called "humanitarian exception" to certain sanctions against the Government of Iran, when in fact no purchases of food or medicine actually occurred. Turkish Bank-1 officials concealed the true nature of these transactions from officials with the U.S. Department of the Treasury so that Turkish Bank-1 could supply billions of dollars' worth of services to the Government of Iran without risking being sanctioned by the U.S. and losing its ability to hold correspondent accounts with U.S. financial institutions.

The International Emergency Economic Powers Act

6. The International Emergency Economic Powers Act ("IEEPA"), codified at Title 50, United States Code, Sections

1701-1706, confers upon the President authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. Section 1705 provides, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this title." 50 U.S.C. § 1705(a).

7. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President found that "the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States and declare[d] a national emergency to deal with that threat."

The Iranian Transactions and Sanctions Regulations

8. On March 15 and May 6, 1995, the President issued Executive Orders Nos. 12957 and 12959, prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person, and on August 19, 1997, issued Executive Order No. 13059 clarifying the previous orders (collectively, the "Executive Orders"). The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations

necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (renamed in 2013, the Iranian Transactions and Sanctions Regulations, the "ITSR") implementing the sanctions imposed by the Executive Orders.

9. The ITSR, Title 31, Code of Federal Regulations, Section 560.204, prohibits, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States Person, of goods, technology, or services to Iran or the Government of Iran (with certain limited exceptions), including the exportation, reexportation, sale or supply of goods, technology or services to a third country knowing that such goods, technology or services are intended for Iran or the Government of Iran, without a license from the United States Department of the Treasury, Office of Foreign Assets Control ("OFAC").

10. The ITSR provide that the transfer of funds, directly or indirectly, from the United States or by a U.S. person to Iran or the Government of Iran is a prohibited export, reexport, sale, or supply of services to Iran or the Government of Iran. See 31 C.F.R. § 560.427(a).

11. The ITSR further prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a

violation of, or attempt to violate the ITSR. 31 C.F.R.

§ 560.203.

**Sanctions Concerning Proceeds of Iranian Oil Sales
and the Supply of Gold to Iran**

12. On December 11, 2011, the National Defense Authorization Act for Fiscal Year 2012 was enacted (the "2012 NDAA"), requiring the imposition of sanctions on foreign financial institutions--including banks and money service business, among others--following a determination by the President that a foreign financial institution violated certain prohibitions with respect to the Central Bank of Iran or another Iranian financial institution designated under the IEEPA. These prohibitions applied to government-owned foreign financial institutions with respect to transactions for the sale or purchase of petroleum or petroleum products to or from Iran conducted or facilitated on or after 180 days from the enactment of the 2012 NDAA, unless the foreign country significantly reduced its volume of petroleum and petroleum products purchased from Iran. These prohibitions included an exception for transactions for the sale of food, medicine, or medical devices to Iran.

13. On July 30, 2012, the President issued Executive Order 13622 to take additional steps with respect to the national emergency declared in Executive Order 12957. The

President, among other things, imposed additional restrictions with respect to the sale of Iranian petroleum and petroleum products, authorizing the Secretary of the Treasury to impose sanctions on a foreign financial institution that knowingly conducted or facilitated any significant financial transaction with NIOC, the Naftiran Intertrade Company Ltd. ("NICO"), or the Central Bank of Iran, or for the purchase or acquisition of petroleum or petroleum products from Iran, unless the President determined the foreign country had significantly reduced its volume of petroleum and petroleum products purchased from Iran pursuant to the 2012 NDAA. Exec. Order 13622, 77 Fed. Reg. 45897 (Jul. 30, 2012).

14. Executive Order 13622 also authorized the Secretary of the Treasury to impose sanctions against any person who "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, NIOC, NICO, or the Central Bank of Iran, or the purchase or acquisition of U.S. bank notes or precious metals by the Government of Iran." Exec. Order 13622, 77 Fed. Reg. 45897 (Jul. 30, 2012). Executive Order 13622 prohibited any transaction that evaded or avoided, had the purpose of evading or avoiding, caused a violation of, or attempted to violate any of the prohibitions set forth in that order.

15. On August 10, 2012, the Iran Threat Reduction and Syria Human Rights Act of 2012, codified at 22 U.S.C. §§ 8711 et seq. (the "Iran Threat Reduction Act" or "ITRA"), extended the sanctions against Iranian oil sales. The ITRA amended the 2012 NDAA by imposing a "bilateral trade" restriction on Iranian oil proceeds: financial transactions by foreign financial institutions with respect to the sale or purchase of petroleum or petroleum products to or from Iran were permitted only for trade between the foreign country and Iran, with any funds owed to Iran deposited in an account within that foreign country. See 22 U.S.C. § 8513a(d)(4)(D). In other words, the proceeds of Iranian oil sales to Turkey had to be deposited into accounts in Turkey and could only be used for trade between Turkey and Iran; otherwise, any foreign financial institution facilitating these transactions faced U.S. sanctions. These requirements went into effect on or about February 6, 2013.

16. On January 2, 2013, the Iranian Freedom and Counterproliferation Act (the "IFCA"), imposed additional restrictions on supplying gold to Iran. The IFCA broadened the prohibition in Executive Order 13622 on supplying precious metals to the Government of Iran to prohibit the sale, supply, or transfer of precious metals, directly or indirectly, to the country of Iran, including non-Government entities. See 22

U.S.C. § 8804(a)(1)(A). The IFCA also extended the ITRA's bilateral trade restriction to the proceeds of Iranian natural gas sales. The IFCA's restrictions went into effect on or about July 1, 2013.

17. On June 3, 2013, the President implemented, among other things, the IFCA's prohibition on dealings in precious metals on behalf of Iran pursuant to his authorities under the IFCA, the IEEPA, and other statutes. Exec. Order 13645, 78 Fed. Reg. 33945 (June 3, 2013). Executive Order 13645 prohibited any transaction that evaded or avoided, had the purpose of evading or avoiding, caused a violation of, or attempted to violate any of the prohibitions set forth in that order.

18. The Secretary of the Treasury promulgated the Iranian Financial Sanctions Regulations (the "IFSR") implementing the sanctions imposed by the Executive Orders 13622 and 13645, the 2012 NDA, the IFCA, and the ITRA, among others. See 31 C.F.R. §§ 561.203, 204, 205. The IFSR prohibited, among other things, transactions that evaded or avoided, had the purpose of evading or avoiding, caused a violation of, or attempted to violate any of the provisions of the IFSR. See 31 C.F.R. § 561.205.

Designated or Identified Entities and Individuals

19. Appendix A to the ITSR contained a list of persons determined to be the Government of Iran. At all times relevant to this Indictment, Bank Mellat was an Iranian state-owned bank on the list in Appendix A. At all times relevant to this Indictment, NIOC was an Iranian Oil Company on the list in Appendix A. At all times relevant to this Indictment, NICO and Naftiran Intertrade Company Sarl ("NICO Sarl") were on the list in Appendix A.

20. At all times relevant to this Indictment, Bank Sarmayeh was an Iranian state-owned bank and, beginning on July 12, 2012, was identified as a state-owned bank by OFAC on the Specially Designated Nationals ("SDN") List. At all times relevant to this Indictment, Sarmayeh Exchange was a money services business in Iran owned and controlled by Bank Sarmayeh.

21. Bank Mellat and all of its branches and subsidiaries were designated by OFAC on or about October 25, 2007, as SDNs under the ITSR, the IFSR, and the Weapons of Mass Destruction Proliferators Sanctions Regulations ("WMD Sanctions"), 31 C.F.R. Part 544. Mellat Exchange Company ("Mellat Exchange") was a money services business owned and controlled by Bank Mellat. At all times relevant to this Indictment, Bank Mellat was an SDN.

22. On or about July 12, 2012, OFAC designated Hong Kong Intertrade Company ("HKICO") as an SDN pursuant to the ITSR. OFAC further identified NIOC as an agent or affiliate of Iran's Islamic Revolutionary Guard Corp ("IRGC") pursuant to Executive Order 13599 on or about September 24, 2012. On or about May 23, 2013, OFAC designated Seifollah Jashnsaz, chairman of NICO, NICO Sarl, and HKICO; Ahmad Ghalebani, managing director of NIOC and a director of both Petro Suisse Intertrade Company SA and HKICO; Farzad Bazargan, managing director of HKICO; Hashem Pouransari, NICO official and managing director of Asia Energy General Trading LLC; and Mahmoud Nikousokhan, NIOC finance director and a director of Petro Suisse Intertrade Company SA as SDNs under the WMD Sanctions. At all times relevant to this Indictment after on or about July 12, 2012, HKICKO was an SDN. At all times relevant to this Indictment after May 23, 2012, Jashnsaz, Ghalebani, Bazargan, Pouransari, and Nikousokhan were each an SDN. At all times relevant to this Indictment after September 24, 2012, NIOC was identified as an agent or affiliate of the IRGC.

23. On or about October 12, 2011, OFAC designated Mahan Air as an SDN pursuant to Executive Order 13224 for providing financial, material and technological support to the Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF").

According to OFAC, Mahan Air, based in Tehran, provided transportation, funds transfers and personnel travel services to the IRGC-QF, including by providing travel services to IRGC-QF personnel flown to and from Iran and Syria for military training, facilitating the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel, facilitated IRGC-QF arms shipments, and received funds for the procurement of controlled goods by the IRGC-QF. Further according to OFAC, Mahan Air also provided transportation services to Hizballah, a Lebanon-based designated Foreign Terrorist Organization, and has transported personnel, weapons, and goods on behalf of Hizballah and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hizballah.

The Defendants

24. At all times relevant to this Indictment, REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, owned and operated a network of companies located in Turkey and in the United Arab Emirates, including a group of companies under Royal Holding A.S. ("Royal Holding"), a holding company in Turkey, and Durak Doviz, a money services business in Turkey later known as Duru Doviz; and did business through the Al Nafees Exchange LLC ("Al

Nafees Exchange"), a money services business in the United Arab Emirates. The Royal Holding group of entities includes Royal Denizcilik, Safir Altin Ticaret, Royal Emerald Investments, among others.

a. ZARRAB and his business associates used high-level contacts in the Turkish and Iranian governments to secure a role in transferring Iranian funds held in Turkey in evasion of U.S. sanctions against Iran. For example, ZARRAB signed a letter written to then-President of Iran Mahmoud Ahmadinejad describing the ZARRAB family's experience in international finance and their willingness and ability to help the Government of Iran defeat U.S. and international sanctions:

Respectfully, at this point in time, when the world-devouring imperialism has been using the weapon of economic blockade and negative propaganda to isolate our beloved homeland, the Islamic Iran, and tightens the grip of sanctions further day-by-day, and considering that serving our beloved nation is a religious duty for every Iranian, in the year of Economic Jihad, under the guidance of the almighty God, hereby the Zarrab family with a half a century of experience in exchange and moving of currency and having been able to set up branches in the United Emirates, Turkey, Russia and Azerbaijan, and doing currency transfers (over three billion euros), sending paper money to Iran (indirectly) and . . . to have a role, however negligible, in serving our beloved homeland, we declare our readiness for any collaboration in moving currency as well as adjusting the rate of exchange under the direct supervision of the

honorable economic agents of the government, within the framework of the international and macroeconomic policies of the blessed regime of the Islamic Republic of Iran, and by using the lease credit facilities and interest.

It is hoped that with the zealous efforts of the children of Islamic Iran we can witness the ever increasing progress of the Islamic homeland and to reach the high summits of respect and honor more than before.

b. ZARRAB and co-conspirators exchanged and reviewed drafts of a similar letter addressed to a senior official of the Central Bank of Iran in December 2011.

25. At all times relevant to this Indictment, MEHMET HAKAN ATILLA, the defendant, was the Deputy General Manager of International Banking at Turkish Bank-1.

26. MEHMET ZAFER CAGLAYAN, the defendant, was the Turkish Minister of the Economy from approximately July 2011 until December 2013 and currently serves in the Turkish Parliament. While Minister of the Economy, CAGLAYAN received tens of millions of dollars' worth of bribes in cash and jewelry from the proceeds of the scheme to provide services to the Government of Iran and to conceal those services from U.S. regulators. CAGLAYAN directed other members of the scheme to engage in certain types of deceptive transactions, approved the steps taken by other members to implement the scheme, and protected the scheme from competitors as well as from scrutiny.

27. SULEYMAN ASLAN, the defendant, was the General Manager of Turkish Bank-1 until approximately February 2014. While General Manager, ASLAN received tens of millions of dollars' worth of bribes in cash from the proceeds of the scheme to provide services to the Government of Iran and to conceal those services from U.S. regulators. In meetings and communications with officials from the U.S. Department of the Treasury, ASLAN concealed the true nature of these transactions so that Turkish Bank-1 could supply billions of dollars' worth of services to the Government of Iran without being sanctioned by the U.S.

28. LEVENT BALKAN, the defendant, was an Assistant Deputy Manager for International Banking at Turkish Bank-1 until approximately February 2013.

29. At all times relevant to this Indictment, ABDULLAH HAPPANI, the defendant, was an associate of REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, working at Durak Doviz and Duru Doviz.

30. At all times relevant to this Indictment, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, owned and operated a network of companies located in Turkey and in the United Arab Emirates, including Flash Doviz ("Flash Doviz"), a money services business in Turkey; Sam

Exchange, a money services business in the UAE; and Hanedan General Trading LLC ("Hanedan General Trading"), a company in the UAE, among others.

31. At all times relevant to this Indictment, CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendant, was an employee of REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, at Royal Holding and related entities.

32. At all times relevant to this Indictment, HOSSEIN NAJAFZADEH, the defendant, was a senior officer at Mellat Exchange.

The Gold Export Scheme

33. As alleged above, in 2012 the United States sanctions relating to the sale of Iranian oil and the supply of currency and precious metals to Iran and the Government of Iran grew more restrictive. In response, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, the defendants, and others devised a scheme to use exports of Turkish gold to allow Iran access to the proceeds of Iranian oil sales to Turkey, to evade these restrictions, and to deceive foreign banks and U.S. regulators.

34. First, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN

ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, CAMELIA JAMSHIDY, a/k/a a/k/a "Kamelia Jamshidy," the defendants, and others conspired to transfer Iranian oil proceeds at Turkish Bank-1 to exchange houses and front companies controlled by ZARRAB in order for those exchange houses and front companies to buy gold for export from Turkey. After being exported from Turkey, the gold could be converted into cash or currency and remitted to Iran or used to conduct international financial transfers on behalf of Iranian persons and entities. Although these gold purchases were made by or on behalf of the Government of Iran, including Iranian banks owned or controlled by the Government of Iran, in violation of Executive Order 13622, ASLAN and ATILLA represented to U.S. Treasury officials that the gold purchases were by private Iranian companies and individuals.

35. Second, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendants, and others conspired to use false documentation and misrepresentations to make it appear that, after gold was purchased in Turkey with the proceeds of Iranian oil sales deposited at Turkish Bank-1, the gold was then exported to Iran when, in fact, the gold was exported to Dubai and sold there, in violation of the ITRA, 22 U.S.C.

§ 8513a(d)(4)(D), in order to obtain U.S. dollars, Euros, and other currencies that could be used to fund the activities of the Government of Iran and Iranian companies and persons.

36. Third, after the IFCA broadened the gold prohibitions to include supply to private Iranian companies and individuals, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, ABDULLAH HAPANI, CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendants, and others conspired to transfer the proceeds of Iranian oil sales held at Turkish Bank-1 to exchange houses and front companies controlled by ZARRAB in order for those exchange houses and front companies to secretly continue buying gold for export from Turkey on behalf of and for the benefit of Iranian persons and companies.

37. REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, arranged meetings in Turkey between approximately October 4 and 8, 2012, among MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, MEHMET HAKAN ATILLA, the defendants, and others, and Iranian government banking and oil officials, including the then-Governor of the Central Bank of Iran and Mahmoud Nikousokhan, then the finance director of NIOC and a director of Petro Suisse Intertrade Company SA. At these meetings the participants discussed, among other things, ZARRAB conducting

financial transfers using the proceeds of Iranian sales of natural gas at Turkish Bank-1 and transferring the proceeds of Iranian sales of oil from China to Turkish Bank-1.

38. On or about October 6, 2012, REZA ZARRAB, a/k/a "Riza Sarraf," and ABDULLAH HAPPANI, the defendants, spoke. During this conversation, ZARRAB told HAPPANI that he just left a meeting with SULEYMAN ASLAN, the defendant, and described an arrangement to pay ASLAN just like ZARRAB already was paying MEHMET ZAFER CAGLAYAN, the defendant. ZARRAB advised, "It's the same arrangement as Abi. You know, it's the same system." HAPPANI asked if CAGLAYAN would be aware of the payments to ASLAN: "If we use the same system, will Abi not know?" ZARRAB informed HAPPANI that CAGLAYAN knew and approved: "I told Abi. He already called me over. He was the one who told me to get it going." "Abi," Turkish for an older brother, was a reference to CAGLAYAN.

39. REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, arranged meetings in Turkey in early May 2013 among MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, the defendants, and others, and Iranian government banking and oil officials, including the then-Iranian Minister of Oil; Ahmad Ghalebani, then the managing director of NIOC; Nikousokhan; and Seifollah Jashnsaz, then the chairman of NICO. At these meetings the

participants discussed, among other things, arranging for the Turkish national oil company to transfer payments for Iranian oil to NIOC at an account held at Turkish Bank-1 by Bank Sarmayeh, an Iranian government-owned bank. ZARRAB had a contract with Sarmayeh Exchange to conduct currency exchange and wire transfers for that entity, giving him preferential access to these Iranian oil revenues.

40. On or about May 6, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," and SULEYMAN ASLAN, the defendants, spoke. During this conversation, ASLAN told ZARRAB that MEHMET HAKAN ATILLA, the defendant, reported that NIOC transferred 70 million (apparently Turkish lira or Euro) directly to an account controlled by ZARRAB at Turkish Bank-1. ZARRAB complained, "No it's not direct, they did it wrong and it will go bank . . . you stop it and I will fix it, they are stupid, they are retarded. . . . Please count that as if it did not happen." ZARRAB later explained that, after ASLAN had left the meeting with the Iranian officials, "we talked and stuff so I would control [that] they wouldn't say something wrong to this they would not say something wrong to that."

41. After IFCA's restrictions on the supply of precious metals to Iran, REZA ZARRAB, a/k/a "Riza Sarraf," continued to use proceeds of Iranian oil and gas sales at

Turkish Bank-1 to buy gold for export from Turkey in order to give the Government of Iran and Iranian persons and companies access to these funds. For example, on or about September 16, 2013, ZARRAB and SULEYMAN ASLAN, the defendant, spoke and, during this conversation, ASLAN reported on a meeting that he recently had with Turkish government officials who asked to increase Turkey's gold exports. ASLAN reported, "the request is, well, they exported \$11 billion in gold last year." ZARRAB responded, "They are asking for the same to be done again, aren't they?" ASLAN replied, "Well, they are saying, 'do something, whatever the method, but help us out, take care of this job,' you know." ASLAN also stated, "I said, 'Iran -- it would not be through Iran, but we -- um, we will find a way, don't you worry.'" ZARRAB responded in part, "We have a method, we will use that. We need to sit down and talk in person."

42. On or about November 11, 2013, a representative of Turkish Bank-1 emailed employees of REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, spreadsheets of transactions relating to exports of gold from Turkey to the United Arab Emirates and Iran that purported to show tens of millions of Euros' worth of gold being exported by Royal Denizcilik and Safir Altin Ticaret to Iran as recently as September and October 2013, including to entities owned and controlled by the Government of Iran.

43. Often REZA ZARRAB, a/k/a "Riza Sarraf," ABDULLAH HAPPANI, CAMELIA JAMSIDY, a/k/a "Kamelia Jamshidy," the defendants, and others caused gold exported from Turkey to be sold in Dubai rather than reexported to the Iranian buyers and the proceeds transferred back to companies owned and controlled by ZARRAB in Turkey, where the proceeds could be further transferred secretly on behalf of and for the benefit of the Government of Iran and Iranian companies and persons. On other occasions, ZARRAB, HAPPANI, JAMSHIDY and others would cause the gold to be re-purchased by companies owned and controlled by ZARRAB in Turkey and imported back to Turkey, where it could be sold. These transactions to sell gold in Dubai or to repurchase and reimport the gold to Turkey on behalf of and for the benefit of the Government of Iran and Iranian companies and persons were often conducted in U.S. dollars. Between at least approximately December 2012 and October 2013, more than \$900 million in such transactions were conducted by U.S. financial institutions through correspondent accounts held in the United States.

The Fraudulent Food and Medicine Trade Scheme

44. In response to the broadened prohibition against the supply of gold to include private Iranian companies and individuals, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN,

ABDULLAH HAPPANI, CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendants, and others also conspired to transfer Iranian oil revenues held at Turkish Bank-1 outside Turkey by falsely pretending that these transfers were in connection with the sale of food and medicine to Iran from Dubai.

45. SULEYMAN ASLAN, MEHMET HAKAN ATILLA, the defendants, and others at Turkish Bank-1 designed the fraudulent food and medicine scheme with REZA ZARRAB, a/k/a "Riza Sarraf," ABDULLAH HAPPANI, the defendants, and others. In addition to designing the scheme, ASLAN and ATILLA concealed the scheme from U.S. Treasury officials in order to avoid potential sanctions against Turkish Bank-1 pursuant to the 2012 NDAA, the ITSR, the IFCA, and the IFSR. MEHMET ZAFER CAGLAYAN, a/k/a "Abi," the defendant, and other Turkish government officials both approved of and directed that the fraudulent food and medicine scheme be adopted and implemented.

46. On or about October 24, 2012, REZA ZARRAB, a/k/a "Riza Sarraf," and LEVENT BALKAN, the defendants, spoke. During that conversation, ZARRAB and BALKAN discussed a transfer of U.S. dollars between ZARRAB's account and Safir Altin's account at Turkish Bank-1. BALKAN warned ZARRAB about the transfer because it was conducted by a U.S. financial institution through its correspondent account in the United States ("U.S. Bank-1").

BALKAN stated, "I mean I'm talking about, one, an American Bank; two, dollars; three, Safir; I mean... many factors are all bundled up here." ZARRAB asked if the transfer would cause an issue, and BALKAN replied, "I just wanted to share it with you. When I mentioned strategic thinking, I meant we should access this together briefly. . . . The balance, the balance is not important. What's more important is security."

47. On or about February 12, 2013, representatives of the U.S. Treasury Department met in Turkey with MEHMET HAKAN ATILLA, the defendant, and other officials of Turkish Bank-1. During this meeting, among other things, the representatives of the U.S. Treasury Department warned Turkish Bank-1 about Iranian attempts to evade sanctions, including through the use of transactions to buy food for import to Iran.

48. On or about March 26, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," and ABDULLAH HAPPANI, the defendants, spoke. During that conversation, ZARRAB and HAPPANI discussed a conversation that ZARRAB just had with SULEYMAN ASLAN, the defendant, about the fact that "they will stop the gold after one-and-a-half months" and that "[h]e [ASLAN] is insisting that we do food and then he will extend it for about two to three months." HAPPANI asked, "How are we going to make it food?", and ZARRAB went on, in part: "He [ASLAN] is saying that we can

send it from Dubai to Iran." ZARRAB later said, "He says that wherever you can provide a document from, do it." ZARRAB later went on to explain, in part: "He [ASLAN] says, 'It's not that, provide it, it is not a problem; whichever way you provide it, provide it. Provide it to Cikinova [coded language meaning false documentation, among other things] and Cikinova will send it; it is not a problem.'"

49. REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, arranged meetings in Turkey between approximately April 9 and 10, 2013, among MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, the defendants, and others, and Iranian government banking and oil officials, including Nikousokhan and Jashnsaz. At these meetings the participants discussed, among other things, designing transactions with the proceeds of Iranian oil sales at Turkish Bank-1 that appeared to be for the purpose of importing food into Iran.

50. On or about July 2, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," and MEHMET HAKAN ATILLA, the defendants, spoke. During that conversation, ZARRAB and ATILLA discussed bills of lading requested by Turkish Bank-1 in connection with ZARRAB's purported food transactions using the proceeds of Iranian oil sales at Turkish Bank-1. ZARRAB explained his purported inability to provide bills of lading because he used small,

five-ton wooden ships for transport between Dubai and Iran that would not provide bills of lading. ATILLA expressed his concern about this explanation: "I'm thinking it would be slightly difficult to carry [goods] weighing 140-150 thousand tons in things that carry five thousand tons." ATILLA later noted, "that's not physically possible." ZARRAB explained that, while he could not provide bills of lading, he could provide customs documents: "The document is being prepared by the government. Customs. Dubai Customs is arranging which ship it will go with, how much, and what's being carried. And also there's the Dubai seal on margin." ATILLA agreed: "You can get those documents? Then give us those documents and I will look at the bill of lading issue later." ZARRAB acknowledged that he had made an error by making the transfer too large: "Hakan, we made an error there. We should have sent it in five million." After further discussion, ZARRAB agreed to also send bills of lading, despite having earlier denied being able to obtain them.

51. On or about July 9, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," and MEHMET HAKAN ATILLA, the defendants, spoke again. During that conversation, ZARRAB and ATILLA discussed, among other things, false supporting documents submitted in connection with ZARRAB's transfers of Iranian oil proceeds at Turkish Bank-1. ATILLA reiterated, "Some of these ships are

very large. There are ships that carry 50,000, 80,000, 90,000 tons of goods. These are not small ships. I beg you to ask our colleagues to take a look at the tonnage." ZARRAB acceded: "Of course. Should they only look at the larger ships?" ATILLA warned of the even greater risks of documents identifying smaller ships:

They should look at the small ones, too. On the larger ships, it's possible to give a bill of lading. On smaller ships, that can carry 13,000, 14,000, the goods are 20,000. That brings attention to these ships. You need to check that out. There are larger goods on the smaller tonnage ships.

ZARRAB asked: "Should I do anything about them?" ATILLA instructed: "They should pay attention that the tonnage should match." ATILLA gave these instructions despite having been earlier informed by Zarrab that the documents he [Zarrab] provided were prepared by Dubai Customs.

52. On or about July 9, 2013, after the call described above in Paragraph 51, REZA ZARRAB, a/k/a "Riza Sarraf," and ABDULLAH HAPPANI, the defendants, spoke. During that conversation, ZARRAB stated, in part, "[T]hese guys loaded 20 thousand tons on a vessel with a capacity of 13 thousand tons; he says to pay attention to these, that's all. The man is just openly saying that don't stick it into our eyes, that's it, what else could he say?" HAPPANI responded, "Thank you, God

bless him, what else can I say?"

53. On or about September 16, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," and SULEYMAN ASLAN, the defendants, spoke. During this conversation, ZARRAB and ASLAN discussed, among other things, the fact that Turkish Bank-1 intended to preclude non-Turkish companies, including two specifically identified American companies, from selling food to Iran in exchange for the proceeds of Iranian oil and gas sales held at Turkish Bank-1 so that ZARRAB would have sole access to these funds.

54. REZA ZARRAB, a/k/a "Riza Sarraf," ABDULLAH HAPPANI, the defendants, and others continued to use fraudulent documentation to represent that transfers of proceeds of Iranian oil and gas sales from Turkish Bank-1 were related to sales of food or medicine. For example, on or about October 14, 2014, ZARRAB sent an email to an official with Turkish Bank-1 attaching documents purportedly relating to the sale of food products by a Dubai company to Iran.

55. On or about October 10, 2014, representatives of the U.S. Department of the Treasury met with MEHMET HAKAN ATILLA, the defendant, and other officials of Turkish Bank-1. During this meeting, representatives of the U.S. Department of the Treasury asked about Turkish Bank-1's dealings with REZA ZARRAB, a/k/a "Riza Sarraf," the defendant. ATILLA denied that

Turkish Bank-1 knowingly participated in any transactions with ZARRAB intended to evade or avoid U.S. sanctions against Iran and claimed to have conducted due diligence on ZARRAB's counterparties.

Scheme To Provide International Wire Transfer Services for the Government of Iran and Iranian Companies and Persons

56. In addition to providing the Government of Iran access to the proceeds of Iranian oil and gas sales deposited at Turkish Bank-1, the defendants also conducted international financial transfers with these proceeds and other funds held for the benefit of Iranian companies and individuals while concealing the true nature of these transfers from banks and U.S. regulators. As a result of this scheme, U.S. financial institutions, among others, were deceived into providing financial services for the benefit of the Government of Iran and Iranian companies and persons that they would not otherwise have provided.

57. Among the Iranian beneficiaries of this scheme were NIOC, NICO, HKICO, Mellat Exchange, Sarmayeh Exchange, and Mahan Air.

Transfers for NIOC, NICO, and HKICO

58. On or about January 7, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, sent an email to a co-conspirator not named as a defendant herein ("CC-1"), an employee of Royal

Holding, attaching instructions for an international financial transfer from Turkish company ECB Kuyumculuk Ic Ve Dis Sanayi Ticaret Limited Sirketi in the amount of approximately \$600,000 to an energy company located in Turkmenistan ("Turkmeni Company-1").

59. On or about January 16, 2013, REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, sent an email to a co-conspirator not named as a defendant herein ("CC-2") attaching a SWIFT message for a payment in the amount of approximately \$1,000,000 from Gunes General Trading LLC, a company located in the U.A.E., to Turkmeni Company-1.

60. On or about January 16, 2013, Gunes General Trading LLC, a co-conspirator not named as a defendant herein, caused an international wire transfer from the U.A.E. to Turkmeni Company-1 in the amount of approximately \$999,907, which was processed by a United States bank ("U.S. Bank-2").

61. On or about November 11, 2013, a co-conspirator not named as a defendant herein ("CC-3") sent an email to REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, attaching (1) a letter from HKICO, signed by Seifollah Jashnsaz and stamped "CONFIDENTIAL," addressed to HKICO's bank concerning an approximately €100 million transfer to HKICO's account; (2) a letter from NIOC concerning an international financial transfer;

and (3) a letter from Turkmeni Company-1 dated May 30, 2013, addressed to the Deputy Minister of Iran's Oil Ministry, instructing that payment to Turkmeni Company-1 be made in U.S. currency.

Transfers for Mellat Exchange

62. On or about January 26, 2011, a co-conspirator not named as a defendant herein ("CC-4"), an employee of Mellat Exchange, described in paragraph 21 above, sent an email to a second co-conspirator not named as a defendant herein ("CC-5"), an employee of Al Nafees Exchange, described in paragraph 25 above, with instructions for Al Nafees Exchange to make international financial transfers on behalf of Mellat Exchange. Included in the instructions was a payment in the amount of approximately \$953,288.85 to a company located in Canada ("Canadian Company-1") described as "transfer by MAPNA." MAPNA was a reference to MAPNA Group, an Iranian construction and power plant company.

63. On or about January 27, 2011, Royal Emerald Investments, a co-conspirator not named as a defendant herein, caused an international wire transfer from the UAE to Canadian Company-1 in the amount of approximately \$953,289, which was processed by a United States bank ("U.S. Bank-3"). The wire transfer information provided to U.S. Bank-3 purported that the

payment was related to fire equipment, but made no mention of MAPNA Group.

64. On or about February 28, 2011, CC-4 of Mellat Exchange sent an email to CC-5 of Al Nafees Exchange with instructions for making several international financial transfers, including four transfers in United States currency, on behalf of Mellat Exchange. Included in the instructions was a payment in the amount of approximately \$76,950 to a company located in China ("Chinese Company-1"), identifying the "Intermediary Bank" for the transaction as a bank located in the United States ("U.S. Bank-4").

65. On or about March 1, 2011, CC-4 sent an email to REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, and to a co-conspirator not named as a defendant herein ("CC-6"), an employee of Royal Holding, attaching a list of the four U.S.-currency payment instructions for Mellat Exchange described in paragraph 64 above.

66. On or about March 9, 2011, CC-4 of Mellat Exchange sent an email to CC-5 of Al Nafees Exchange with instructions for making several international financial transfers in United States currency on behalf of Mellat Exchange. Included in the instructions was a payment in the amount of approximately \$9,225 to a company located in Hong Kong

("Hong Kong Company-1").

67. On or about May 24, 2011, CC-4 of Mellat Exchange sent an email to REZA ZARRAB, a/k/a "Riza Sarraf," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendants, and CC-6 of Royal Holdings with the subject line, in Farsi, "very very urgent!!!!!!!!!!!!" Attached to the email were (1) a portion of a SWIFT message addressed to the attention of "OFAC/Compliance Unit" indicating that an international wire transfer in the amount of approximately €3,711,365 had been stopped by U.S. Bank-3 because of global sanctions; (2) a statement that the payment related to services provided in connection with development of a gas field in Iran; and (3) a letter from Mellat Exchange to ZARRAB stating in part, in Farsi:

Based on the results of the continuous follow-ups regarding the above transfer, and your suggestion regarding communication with the OFAC agency in Turkey regarding facilitating transfers or returns thereof, the information received from the credit applicant is reflected exactly for follow up and appropriate action.

68. On or about May 31, 2011, CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," the defendant, sent an email to CC-5 of Al Nafees Exchange attaching a letter from Mellat Exchange, signed by HOSSEIN NAJAFZADEH, the defendant, to Al Nafees Exchange requesting the delivery of approximately \$30 million in U.S. currency to Mellat Exchange in Tehran, Iran.

69. On or about June 1, 2011, CC-4 of Mellat Exchange sent an email to REZA ZARRAB, a/k/a "Riza Sarraf," the defendant, with the subject line, in Farsi, "very urgent" and attaching, among other things, (1) a portion of a SWIFT message noting that a payment in the amount of approximately \$9,225 had been blocked by U.S. Bank-1 "pursuant to the sanctions imposed by the U.S. Gov Dept. of Treasury OFAC"; (2) a letter from Hong Kong Company-1's bank advising that a payment to Hong Kong Company-1 from Asi Kiyetli Madenler Turizm Otom in the amount of approximately \$9,200 had been blocked by U.S. Bank-1 because of OFAC; (3) a portion of a second SWIFT message noting that payment of a second international transfer to Hong Kong Company-1 in the amount of approximately \$35,000 had been blocked by a United States bank ("U.S. Bank-5") as a result of OFAC sanctions; (4) a letter from Mellat Exchange dated May 15, 2011, to a relative of ZARRAB's at Al Nafees Exchange, signed by HOSSEIN NAJAFZADEH, the defendant, concerning the two blocked payments; and (5) a letter from Mellat Exchange dated June 1, 2011, to Durak Doviz, signed by NAJAFZADEH, concerning the two payments "through the Nafees Exchange," which stated in part, in Farsi:

[T]he above amounts were blocked by OFAC, and despite repeated follow-ups to execute these transfers by providing all necessary documents, unfortunately, the transfers have

not been executed and deposited in the beneficiary's account. Therefore, despite the lack of communication with you regarding the covered topic, and only with regard to your excellent achievements regarding similar prior cases, it is requested: Regarding the passage of more than 2 months, and the lack of any results from the follow-ups of Nafiss Exchange, please arrange that with your guidance this case can be closed.

Transfers for Mahan Air

70. On or about October 13, 2011, a co-conspirator not named as a defendant herein ("CC-7"), an individual affiliated with Mahan Air's office in Dubai, received an email from a representative of Mahan Air with the subject "IMPORTANT !! -- MAHAN AIR has been OFAC listed from US Treasury Department" and including, among other things, a statement that a bank had advised that "all transactions to/from Mahan Air will be rejected as per sanctions policy, following the addition of Mahan Air to the OFAC list[.]"

71. On or about December 18, 2013, CC-5 received an email from an employee of the Al Nafees Exchange with the subject line: "ASCOT" and attaching electronic copies of (1) license information for Ascot General Trading, a Dubai company, showing CC-7 as the licensee and manager, on which was a handwritten note in Farsi referencing "Mahan" and the name of an officer in Mahan Air's Dubai office, a co-conspirator not named as a defendant herein ("CC-8"); (2) pages from the

passport of CC-7; (3) an Al Nafees Exchange account signature card for Ascot General Trading showing CC-7 as the account signatory; and (4) a letter dated December 17, 2013, on Ascot General Trading letterhead, signed by CC-7 and addressed to Al Nafees Exchange, directing a transfer from Ascot General Trading's account to a beneficiary with an account at an Iranian bank.

72. On or about January 19, 2015, CC-7 received an email from a money services business advising that a wire transfer had been returned, and including a portion of a SWIFT message stating, among other things, "ORIGINATOR IN OFAC SANCTIONLIST."

73. On or about June 25, 2015, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, received an email from an employee of the Al Nafees Exchange attaching an electronic copy of an Al Nafees Exchange Payment Order for Flash Doviz, MOHAMMAD ZARRAB's company, concerning a payment of \$1,180,238.00 (U.S. dollars) and a second payment of €129,901.00 from Ascot General Trading to Flash Doviz "FOR MAHAN" and naming CC-8. A handwritten note on the payment order, in Farsi, read in part: "Please deposit the above amounts in the Mahan account and show us the transfer slips."

74. On or about July 6, 2015, CC-5 sent an email to

MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, attaching electronic copies of (1) an Al Nafees Exchange Payment Order for Flash Doviz concerning a payment of approximately €570,613.00 from Ascot General Trading to Flash Doviz "FOR MAHAN" and naming CC-8, with a handwritten note in Farsi that read: "Should be deposited into the Mahan account with you;" and (2) four Funds Transfer Request Forms concerning requested payments totaling approximately €560,613 to recipients in Austria, Greece, Singapore, and Germany, each bearing an Ascot General Trading stamp.

75. On or about July 7 and July 8, 2015, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, sent CC-5 approximately four emails attaching electronic copies of wire transfer records concerning payments corresponding to the Funds Transfer Requests that CC-5 had sent to MOHAMMAD ZARRAB on or about July 6, 2015. The originators on the wire transfers were two Turkish companies ("Turkish Company-1" and "Turkish Company-2").

76. On or about July 9, 2015, CC-5 sent two emails to an officer with Mahan Air, a co-conspirator not named as a defendant herein ("CC-9"), attaching the wire transfer records that CC-5 had received from MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, on July 7 and July 8, 2015.

77. On or about July 13, 2015, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, sent CC-5 an email attaching an electronic copy of a SWIFT message concerning a transfer of \$324,690 from Turkish Company-1 to a company in Malaysia ("Malaysian Company-1"). The SWIFT message record reflected that the message had been sent from a bank in Turkey to U.S. Bank-4 in "New York, NY, United States of America," indicating that the payment would be transferred through a correspondent account held at U.S. Bank-4.

78. On or about July 21, 2015, CC-5 sent an email to MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, with the subject: "tt's" -- a reference to telegraphic transfers, or wire transfers. Attached to the email was an Al Nafees Exchange Payment Order concerning four payments from Ascot General Trading to Flash Doviz for Mahan Air in the amounts of \$116,385, €363,971, \$100,000, and €298,984. A handwritten note on the payment order read, in Farsi, "Put in the Mahan account." Also attached to the email were four Fund Transfer Request Forms, bearing an Ascot General Trading stamp, concerning payments (1) to a company in Hong Kong ("Hong Kong Company-2") for \$100,000, and (2) an entity purportedly located in Belize (but having an account in Latvia) and entities located in Greece and Belgium in the amounts of €363,971, €75,524, and

€45,208, respectively.

79. On or about July 22, 2015, an email was sent from an employee of MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, a co-conspirator not named as a defendant herein ("CC-10"), to CC-5 attaching an electronic copy of a Wire Transfer Send Money Receipt from a money services business in Dubai reflecting a wire transfer of \$100,000 from Hanedan General Trading to Hong Kong Company-2.

80. On or about July 23, 2015, CC-5 sent an email to MOHAMMAD ZARRAB attaching electronic copies of (1) an Al Nafees Exchange Payment Order concerning transfers (a) from Ascot General Trading to a co-conspirator not named as a defendant herein ("CC-11"), an employee of MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," the defendant, in the amount of €200,000, (b) to Flash Doviz for Mahan Air in the amount of €87,520, and (c) to Flash Doviz for Mahan Air in the amount of \$50,000; and (2) Ascot General Trading Funds Transfer Requests concerning payments to Hong Kong Company-2 in the amount of \$50,000 and to entities located in France and Germany for €27,520 and €60,000, respectively.

81. On or about July 23, 2015, CC-7 sent an email to CC-5 with the subject: "Re: 100.000,00 USD MAHAN AIR" and attaching an electronic copy of a wire transfer record

reflecting a transfer in the amount of approximately \$99,940.00 from Hanedan General Trading to Hong Kong Company-2 and identifying the intermediary bank for the transfer as U.S. Bank-4 in "New York, NY USA."

82. Later on July 23, 2015, CC-5 sent an email to CC-9 attaching an electronic copy of the wire transfer record described in paragraph 81 above, with portions of the information blacked out but reflecting, among other things, the originator, beneficiary, and intermediary bank (U.S. Bank-1).

83. On or about July 27, 2015, CC-7 sent an email to CC-5 attaching an electronic copy of a Wire Transfer Send Money Receipt from a money services business in Dubai reflecting a wire transfer of \$50,000 from Hanedan General Trading to Hong Kong Company-2.

84. On or about July 29, 2015, CC-7 sent an email to CC-5 with the subject: "Re: 50.000,00 USD MAHAN AIR" and attaching an electronic copy of a wire transfer record reflecting a transfer in the amount of approximately \$49,950.00 from Hanedan General Trading to Hong Kong Company-2, and identifying the intermediary bank for the transfer as U.S. Bank-1 in "New York, NY USA."

STATUTORY ALLEGATIONS

COUNT ONE

(Conspiracy to Defraud the United States)

The Grand Jury charges:

85. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

86. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to defraud the United States and an agency thereof, to wit, to impair, impede, and obstruct the lawful and legitimate governmental functions and operations of the U.S. Department of the Treasury in the enforcement of economic sanctions laws and regulations administered by that agency.

Overt Acts

87. In furtherance of the conspiracy and to effect the illegal object thereof, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others committed the overt acts set forth in paragraphs 33 to 84 of this Indictment, among others, which are fully incorporated by reference herein.

(Title 18, United States Code, Section 371.)

COUNT TWO

(Conspiracy to Violate the

International Emergency Economic Powers Act)

The Grand Jury further charges:

88. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

89. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH

HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to violate, and to cause a violation of, licenses, orders, regulations, and prohibitions issued under the International Emergency Economic Powers Act.

90. It was a part and an object of the conspiracy that REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, would and did provide and cause others to provide financial services to Iran and to the Government of Iran prohibited by U.S. law, without first obtaining the required approval of OFAC, and to evade and avoid the requirements of U.S. law with respect to the provision of financial services to Iran and to the Government of Iran, in violation of Executive Orders 12959, 13059, 13224, 13599, 13622, and 13645 and 31 C.F.R. §§ 560.203, 560.204, 560.205, 561.203, 561.204, and 561.205.

(Title 50, United States Code, Section 1705;

Executive Orders 12959, 13059, 13224, 13599, 13622, and 13645;
Title 31, Code of Federal Regulations, Sections 560.203,
560.204, 560.205, 561.203, 561.204 & 561.205.)

COUNT THREE

(Bank Fraud)

The Grand Jury further charges:

91. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

92. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, did knowingly execute and attempt to execute a scheme or artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation ("FDIC"), and to obtain moneys, funds, credits, assets, securities, and other property owned by and under the custody and control of such financial institution, by means of false and fraudulent pretenses, representations, and promises, and aided and abetted

the same, to wit, inducing U.S. financial institutions to conduct financial transactions on behalf of and for the benefit of the Government of Iran and Iranian entities and persons using money and property owned by and under the custody and control of such financial institutions, by deceptive means.

(Title 18, United States Code, Sections 1344 & 2.)

COUNT FOUR

(Conspiracy to Commit Bank Fraud)

The Grand Jury further charges:

93. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

94. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to

commit bank fraud, in violation of Title 18, United States Code, Section 1344.

95. It was a part and an object of the conspiracy that REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, would and did knowingly execute and attempt to execute a scheme or artifice to defraud a financial institution, the deposits of which were then insured by the FDIC, and to obtain moneys, funds, credits, assets, securities, and other property owned by and under the custody and control of a financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

(Title 18, United States Code, Section 1349.)

COUNT FIVE

(Money Laundering)

The Grand Jury further charges:

96. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

97. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, together with others known and unknown, in an offense involving and affecting interstate and foreign commerce, did knowingly transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds to places in the United States from and through places outside the United States, in amounts exceeding \$10,000, and aided and abetted the same, with the intent to promote the carrying on of specified unlawful activity, to wit, (i) the illegal export of services to Iran as charged in Count Two of this Indictment, (ii) bank fraud as charged in Counts Three and Four of this Indictment, and (iii) an offense against a foreign nation involving bribery of a public official.

(Title 18, United States Code, Sections 1956(a)(2)(A) & 2.)

COUNT SIX

(Conspiracy to Commit Money Laundering)

The Grand Jury further charges:

98. The allegations contained in paragraphs 1 through 84 of this Indictment are repeated and realleged as if fully set forth herein.

99. From at least in or about 2010, up to and including in or about 2015, in the Southern District of New York, Turkey, the United Arab Emirates, and elsewhere, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, together with others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to violate Title 18, United States Code, Section 1956(a)(2)(A).

100. It was a part and an object of the conspiracy that REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy,"

and HOSSEIN NAJAFZADEH, the defendants, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds to places in the United States from and through places outside the United States, in amounts exceeding \$10,000, with the intent to promote the carrying on of specified unlawful activity, to wit, (i) the illegal export of services to Iran as charged in Count Two of this Indictment, (ii) bank fraud as charged in Counts Three and Four of this Indictment, and (iii) an offense against a foreign nation involving bribery of a public official, in violation of Section 1956(a)(2)(A) of Title 18, United States Code.

(Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATION

(Counts Two, Three, and Four)

101. As a result of committing the offenses alleged in Counts Two, Three, and Four of this Indictment, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, shall forfeit to the United States, pursuant to

Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offenses alleged in Counts Two, Three, and Four of this Indictment, including but not limited to a sum of money representing the amount of proceeds obtained as a result of the offenses.

Substitute Assets Provision

102. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a) cannot be located upon the exercise of due diligence;
- b) has been transferred or sold to, or deposited with, a third person;
- c) has been placed beyond the jurisdiction of the court;
- d) has been substantially diminished in value; or
- e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

FORFEITURE ALLEGATION

(Counts Five and Six)

103. As a result of committing the money laundering offenses alleged in Counts Five and Six of this Indictment, REZA ZARRAB, a/k/a "Riza Sarraf," MEHMET HAKAN ATILLA, MEHMET ZAFER CAGLAYAN, a/k/a "Abi," SULEYMAN ASLAN, LEVENT BALKAN, ABDULLAH HAPPANI, MOHAMMAD ZARRAB, a/k/a "Can Sarraf," a/k/a "Kartalmsd," CAMELIA JAMSHIDY, a/k/a "Kamelia Jamshidy," and HOSSEIN NAJAFZADEH, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982, all property, real and personal, involved in the money laundering offenses and all property traceable to such property, including but not limited to, a sum of money representing the amount of property that was involved in the money laundering offenses or is traceable to such property.

Substitute Assets Provision

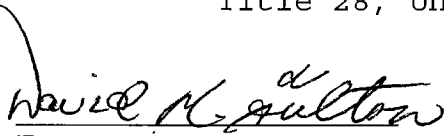
104. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a) cannot be located upon the exercise of due diligence;
- b) has been transferred or sold to, or deposited with, a third person;
- c) has been placed beyond the jurisdiction of the court;

- d) has been substantially diminished in value;
or
- e) has been commingled with other property
which cannot be subdivided without
difficulty;

it is the intent of the United States, pursuant to Title 21,
United States Code, Section 853(p), to seek forfeiture of any
other property of said defendants up to the value of the above
forfeitable property.

(Title 18, United States Code, Sections 981, 982;
Title 21, United States Code, Section 853;
Title 28, United States Code, Section 2461.)



Foreperson



JOON H. KIM
Acting United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

REZA ZARRAB, a/k/a "Riza Sarraf,"
MEHMET HAKAN ATILLA,
MEHMET ZAFER CAGLAYAN, a/k/a "Abi,"
SULEYMAN ASLAN,
LEVENT BALKAN,
MOHAMMAD ZARRAB, a/k/a "Can Sarraf,"
a/k/a "Kartalmsd,"
CAMELIA JAMSHIDY, a/k/a "Kamelia
Jamshidy," and
HOSSEIN NAJAFZADEH,

Defendants.

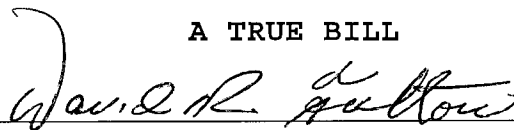
SUPERSEDING INDICTMENT

S4 15 Cr. 867 (RMB)

(18 U.S.C. § 371; 50 U.S.C. § 1705; 31
C.F.R. §§ 560.203, 560.205, 561.203,
561.204, 561.205; 18 U.S.C. §§ 1349,
1956, & 2.)

JOON H. KIM
Acting United States Attorney.

A TRUE BILL



Foreperson.

9/6/17

Filed Indictment
Arrest Warrants ordered

USMJ Parker



EXHIBIT J

ELECTRONICALLY FILED

DOC #:

DATE FILED: MAR 19 2017

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -x
:
UNITED STATES OF AMERICA
:
- v. -
:
ALI SADR HASHEMI NEJAD,
:
Defendant.
:
- - - - -x

SEALED INDICTMENT

18 CRIM 224

JUDGE CARTER

BACKGROUND

The International Emergency Economic Powers Act

The Grand Jury charges:

1. The International Emergency Economic Powers Act ("IEEPA"), codified at Title 50, United States Code, Sections 1701-1706, confers upon the President authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. Section 1705 provides, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this title." 50 U.S.C. § 1705(a).

2. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President found that "the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United

States and declare[d] a national emergency to deal with that threat."

3. On May 6, 1995, the President issued Executive Order No. 12959, adopting and continuing Executive Order No. 12170 (collectively, the "Executive Orders"), and prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person. The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (renamed in 2013, the Iranian Transactions and Sanctions Regulations, the "ITSR") implementing the sanctions imposed by the Executive Orders.

4. The ITSR, Title 31, Code of Federal Regulations, Section 560.204, prohibits, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States Person, of goods, technology, or services to Iran or the Government of Iran (with certain limited exceptions), including the exportation, reexportation, sale or supply of goods, technology or services

to a third country knowing that such goods, technology or services are intended for Iran or the Government of Iran, without a license from the United States Department of the Treasury, Office of Foreign Assets Control ("OFAC").

5. The ITSR further prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate the ITSR. 31 C.F.R. § 560.203.

The Venezuelan Housing Project and the Defendant

6. On or about August 31, 2004, the Governments of Venezuela and Iran entered into a Cooperation Framework Agreement, whereby they agreed to cooperate in certain areas of common interest. On or about December 2, 2005, the Governments of Venezuela and Iran supplemented the Cooperation Framework Agreement by entering into a Memorandum of Understanding (the "MOU") regarding an infrastructure project in Venezuela (the "Project"). Together, those agreements, in substance and in part, called for cooperation between the Governments of Venezuela and Iran toward the construction of thousands of housing units in Venezuela by, for example, directing the parties to sign "commercial contracts" for the purpose of completing the Project.

7. The Project was led by Stratus Group, an Iranian

conglomerate established in Tehran, Iran, in or about 1978 with business operations in the construction, banking, and oil industries. Among other entities, Stratus Group comprises Stratus International Contracting Company, a Tehran-based construction company, which has developed infrastructure projects in Iran and elsewhere, including in Yemen, Pakistan, and Djibouti, as well as the Eghtesad-e-Novin Bank ("EN Bank"), which was the first private bank in Iran. At all times relevant to this Indictment, Stratus Group was controlled and operated by a co-conspirator not named as a defendant herein ("CC-1") and CC-1's family, including CC-1's son, ALI SADR HASHEMI NEJAD, the defendant.

8. In or about December 2006, Stratus Group incorporated a company in Tehran, which was then-known as the Iranian International Housing Corporation ("IIHC"). IIHC was responsible for construction for the Project. At all times relevant to this Indictment, IIHC was owned and operated by the Stratus Group.

9. On or about July 2, 2007, IIHC entered into a contract with a subsidiary (the "Subsidiary") of a Venezuelan state-owned energy company (the "VE Company"), which called for IIHC to build approximately 7,000 housing units in Venezuela in exchange for approximately \$475,734,000 U.S. dollars.

10. In or about 2009, the Stratus Group created the Venezuela Project Executive Committee (the "Project Committee") to oversee the execution of the Project. Its members included, among others, ALI SADR HASHEMI NEJAD, the defendant. The defendant also had other roles in connection with the Project. For example, SADR was responsible for managing the Project finances.

11. In or about 2010, ALI SADR HASHEMI NEJAD, the defendant, and CC-1 incorporated two entities outside Iran, using St. Kitts and Nevis passports and a Dubai, United Arab Emirates address, for the purpose of, *inter alia*, receiving U.S. dollar ("USD") payments related to the Project on behalf of IIHC: (i) Clarity Trade and Finance ("Clarity"), which was incorporated in Switzerland on or about March 19, 2010, and (ii) Stratus International Contracting, J.S., a/k/a "Stratus Turkey," a/k/a "Straturk" ("Stratus Turkey"), which was incorporated in Turkey on or about October 20, 2010. At all times relevant to this Indictment, Stratus Turkey and Clarity were owned and controlled by SADR and his family members.

12. At all times relevant to this Indictment, ALI SADR HASHEMI NEJAD, the defendant, and others conspired to evade U.S. sanctions by conducting international financial transactions using Clarity and Stratus Turkey on behalf of and

for the benefit of Iranian individuals and entities, including themselves and IIHC, in order to conceal from U.S. banks and others that services were being provided to Iran in violation of the IEEPA and the ITSR.

13. Specifically, between in or about April 2011 and in or about November 2013, the VE Company, at the direction of ALI SADR HASHEMI NEJAD, the defendant, and others, made approximately fifteen payments to IIHC on behalf of the Subsidiary through Stratus Turkey or Clarity, totaling approximately \$115,000,000 USD. As directed by the defendant, and others, the payments were routed from the VE Company through banks in the United States to Stratus Turkey or Clarity's bank accounts at a financial institution in Switzerland ("Swiss Bank-1"). Once the payments were received by Stratus Turkey and Clarity, the majority of the funds were transferred to another off-shore entity located in the British Virgin Islands which was incorporated by SADR and others, on or about February 2, 2009. Additionally, on or about February 1, 2012, Clarity wired more than \$2,000,000 of proceeds from the Project directly into the United States. Those proceeds were then used to purchase real property in California.

STATUTORY ALLEGATIONS

COUNT ONE

(Conspiracy to Defraud the United States)

The Grand Jury further charges:

14. The allegations contained in paragraphs 1 through 13 of this Indictment are repeated and realleged as if fully set forth herein.

15. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to defraud the United States and an agency thereof, to wit, to impair, impede, and obstruct the lawful and legitimate governmental functions and operations of OFAC in the enforcement of economic sanctions laws and regulations administered by that agency.

Overt Acts

16. In furtherance of the conspiracy and to effect the illegal object thereof, ALI SADR HASHEMI NEJAD, the defendant, and others committed the overt acts set forth below, among others:

a. On or about February 2, 2009, CC-1 incorporated Stratus Global Investments Incorporated in St. Kitts and Nevis.

b. On or about December 8, 2009, CC-1 incorporated Cirrus General Trading FZE ("Cirrus") in Dubai, United Arab Emirates.

c. On or about February 10, 2010, IIHC nominated Cirrus to receive the proceeds of the Project on its behalf.

d. On or about February 22, 2010, CC-1 registered Clarity Trade & Finance, S.A. in Switzerland and opened a temporary bank account in Clarity's name at a financial institution in Switzerland ("Swiss Bank-2").

e. On or about March 19, 2010, SADR incorporated Clarity in Switzerland.

f. On or about May 12, 2010, Cirrus received approximately 11,388,566 Euros at its bank account at a financial institution located in Dubai ("UAE Bank-1") representing a payment for the first invoice related to the Project.

g. On or about May 31, 2010, SADR opened bank accounts in the name of Clarity at Swiss Bank-1.

h. On or about July 30, 2010, SADR sent an email to CC-1 stating, in substance and in part: "Please find attached a copy of Caliry's [sic] USD and EUR accounts in order to shift our deposit routes" Attached to that email were documents reflecting Clarity's USD account information at Swiss Bank-1 and listing a U.S.-based bank in New York, New York ("U.S. Bank-1") as the intermediary bank for USD transfers.

i. On or about October 20, 2010, CC-1 and SADR incorporated Stratus International Contracting Insaat Ve Taahhut Anonim Sirketi ("Stratus Turkey") in Istanbul, Turkey, listing St. Kitts and Nevis as their individual nationality and providing a Dubai personal address. Under the articles of incorporation, CC-1, SADR, and SADR's sister ("Sister-1") owned 90% of the shares of Stratus Turkey, and another co-conspirator ("CC-2") owned 4% of the shares.

j. On or about October 28, 2010, SADR opened a bank account in the name of Stratus Turkey at Swiss Bank-1, stating "I shall be the sole signatory on the account for now, till I add my father and sister later on."

k. On or about December 30, 2010, SADR sent an email to a co-conspirator not named as a defendant herein ("CC-3") stating, "Please find attached the USD account information as requested" and attaching a document listing Stratus Turkey as

the "Beneficiary," Swiss Bank-1 as the "Bank of Beneficiary," and U.S. Bank-1, located in New York, New York, as the "Intermediary Bank."

1. On or about February 2, 2011, SADR sent an email to an employee at Swiss Bank-1 stating, "We are expecting \$29m in the coming couple of weeks from Venezuela, so please have your watchful eye on that."

m. On or about February 11, 2011, CC-3 sent an email to SADR requesting that SADR "[p]lease reconfirm the information of account in USD." Attached to the email was a draft letter in the name of another co-conspirator not named as a defendant herein ("CC-4") on "Iranian Intl. Housing Co." letterhead, with an address in Tehran, Iran, stating in part, "In the view of current difficulties for transfer and movement of funds and to facilitate the process we have decided to appoint a company in Istanbul - Turkey (Stratus International Contracting Insaat ve Taahhut A.S.) to act as our agent and propose to make the payment of IPCs [engineering, procurement, and construction invoices] through this agent." The letter further stated, "For USD:" and listed U.S. Bank-1 in New York, New York, as the correspondent bank, Swiss Bank-1 as the "Bank of Beneficiary," and Stratus Turkey as the "Beneficiary".

n. On or about February 12, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Stratus Turkey for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Stratus International Contracting Insaat ve Taahhut A.S. to act as our agent for receiving the payment of IPCs. Therefore, we, hereby, request you to order to make the payment of IPCs 7, 8, 9, and 10 to the account of the aforementioned company with the below details." The letter further stated, "For USD:" and listed U.S. Bank-1 in New York, New York, as the correspondent bank, Swiss Bank-1 as the "Bank of Beneficiary," and Stratus Turkey as the "Beneficiary" with "Purpose of payment: Valuation Number 7 to 10 of Fabricio Ojeda New City, Urban Project."

o. On or about March 7, 2011, SADR sent an email to CC-4, stating, in substance and in part, that IIHC will be using an abbreviated version of its full business name in Venezuela "so that we can make our transactions a bit easier," and because "we have requested our last invoice to be paid in USD which makes this name change a bit more crucial." Attached

to that email were minutes of an "Extraordinary General Meeting" of the Project Committee, including CC-1, CC-3, and others, during which they discussed, among other things, using the abbreviated name because they were now requesting payments in USD.

p. On or about March 26, 2011, SADR sent an email to CC-3 stating, in substance and in part, that CC-3 should inform the "client" that "[t]here's no Iranian behind any accounts" that relate to the Project.

q. On or about April 4, 2011, the Subsidiary caused an international wire transfer to Swiss Bank-1 on behalf of Stratus Turkey, in the amount of approximately \$29,442,967.57 for IPCs 7, 8, 9, and 10, which was processed by U.S. Bank-1.

r. On or about May 9, 2011, CC-2 sent an email to SADR with the subject line "restructuring of Stratus International Turkey," stating, in substance and in part:

Confirmed that either 5 persons or combination of persons and legal entities with a minimum number 5 required. Therefore, 1 Austrian company is not sufficient. 4 more persons or legal entities should be added to the new structure. Since we, none of us want our individual names to be shown in the structure due to the reasons in Venezuela and Iran, we have to find 4 more legal entities or names for the minor shares.

s. On or about June 14, 2011, CC-2 sent an email to SADR, copying CC-4, stating in substance and in part,

"Further to our last conversation, I attach the final letter ready for signing and submission. Since it is too late in Tehran . . . I would like to get your agreement to produce [CC-4's] signature." Attached to the email was a draft letter on IIHC letterhead to the Subsidiary, requesting payment for IPCs 11-13.

t. On or about July 1, 2011, SADR and CC-2 caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to conduct an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In the view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPCs [11, 12, and 13]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

u. On or about July 2, 2011, CC-2 emailed CC-4, copying SADR stating in substance and in part, "Please accept my apologies first of all for being used [sic] your signature for the attached letter," and attached the July 1, 2011 IIHC letter to the Subsidiary requesting payment for IPCs 11, 12, and 13.

v. On or about July 5, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$20,692,579.48 for IPCs 11, 12, and 13, which was processed by U.S. Bank-1.

w. On or about July 6, 2011, SADR sent CC-2 an email stating, in substance and in part, "Please find attached the swift confirmation for the incoming funds from Venezuela for the amount of USD20,692,579.48. It seems like our strategy has worked so far."

x. On or about July 22, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPC[14]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

y. On or about August 11, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account

at Swiss Bank-1, in the amount of approximately \$5,418,765.49 for IPC 14, which was processed by U.S. Bank-1.

z. On or about September 27, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPCs [15 and 16]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

aa. On or about October 12, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$5,874,779.37 for IPCs 15 and 16, which was processed by U.S. Bank-1.

bb. On or about October 17, 2011, CC-2 sent an email to a co-conspirator not named as a defendant herein ("CC-5") stating, in substance and in part, that IIHC will change its name from Iranian International Housing Company to International

Housing Company "[d]ue to developing circumstances." CC-2 forwarded the email to SADR.

cc. On or about October 24, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPCs [17 and 18]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

dd. On October 24, 2011, SADR sent an email to CC-2, responding to CC-2's email recommending, in substance and in part, to change IIHC's name to either "International Industrial Housing Company" or "International Iron Housing Company," and stating, in substance and in part, "I think the first choice is a good one," but that the order should be "Industrial International Housing Company."

ee. On or about November 9, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$12,904,173.50 for IPCs 17 and 18, which was processed by U.S. Bank-1.

ff. On or about November 12, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPC [19]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary.".

gg. On or about November 28, 2011, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we

already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPC [20]." The letter provided the following payment instruction details: U.S. Bank-1 in New York, New York, as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

hh. On or about December 27, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$4,243,372.66 for IPC 19, which was processed by U.S. Bank-1.

ii. On or about December 30, 2011, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$6,704,753.09 for IPC 20, which was processed by U.S. Bank-1.

jj. On or about January 5, 2012, an assistant to SADR and CC-2 sent CC-2 an email, copying SADR, and attaching new payment routing instructions for future USD payment to Clarity's account at Swiss Bank-1. The instructions listed another financial institution based in Switzerland ("Swiss Bank-3") as the new "Intermediary Bank" for USD payments.

kk. On or about January 26, 2012, SADR, CC-2, and CC-3 caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of

IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPC [21]." The letter provided the following payment instruction details: Swiss Bank-3 as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary."

ll. On or about February 23, 2012, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$7,389,475.00 for IPC 21, which was processed by another U.S.-based bank ("U.S. Bank-2"), in New York, New York.

mm. On or about April 13, 2012, the Subsidiary caused an international wire transfer to Clarity's bank account at Swiss Bank-1, in the amount of approximately \$15,776,884.74, which was processed by U.S. Bank-2 in New York, New York.

nn. On or about May 30, 2012, SADR and CC-3 caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "In view of the current difficulties for

transfer and movements of funds and to facilitate the process we already appointed Clarity Trade & Finance S.A. to act as our agent for receiving the payment of IPCs [23 and 24]." The letter provided the following payment instruction details: U.S. Bank-2 as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Clarity as the "Beneficiary".

oo. In or about August 2012, CC-3 visited an official representative of the Iranian government in Caracas, Venezuela ("Iranian Government Official-1") and asked, in substance and in part, for diplomatic intervention regarding payments owed to IIHC pursuant to the Project.

pp. On or about August 31, 2012, SADR, CC-3, and others caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Clarity for the benefit of IIHC. The letter, which was on IIHC letterhead, included the following language: "Referring to our meeting held in the Miranda Building date on 30.08.2012 we hereby according to the minutes of the said meeting request you to order to make the payment for IPC 23 & 24 to the following accounts with the below details, in USD currency and in BsF [Venezuelan Bolivars]." The letter provided the following payment instruction details for USD payment: U.S. Bank-2 as the "Intermediary Bank," Swiss Bank-

1 as the "Beneficiary's Bank," and Stratus Turkey as the "Beneficiary." For Bolivar payments, the letter listed IIHC as the beneficiary with an account at a financial institution in Venezuela ("Venezuela Bank-1").

qq. On or about September 21, 2012, the Subsidiary caused an international wire transfer to a Stratus Turkey bank account at Swiss Bank-1, in the amount of approximately \$1,894,333.40 for IPCs 23, 24, and 25, which was processed by U.S. Bank-2.

rr. On or about September 27, 2012, a co-conspirator not named as a defendant herein ("CC-6") sent an email to CC-2, copying SADR, stating, in substance and in part, "we received USD 1,894,333.40 into our Stratus Intl. account from Venezuela."

ss. On or about October 15, 2012, SADR and CC-3 caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Stratus Turkey for the benefit of IIHC. The letter, which was on IIHC letterhead, requested payment in both USD and Bolivars for IPCs 26, 27, 28, and 29, and provided the following payment instruction details for USD payment: U.S. Bank-2 as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Stratus Turkey as the

"Beneficiary." For Bolivar payments, the letter listed IIHC as the beneficiary with an account at Venezuelan Bank-1.

tt. On or about November 14, 2012, the Subsidiary caused an international wire transfer to Stratus Turkey's bank account at Swiss Bank-1, in the amount of approximately \$1,238,741.38 for IPC 26, which was processed by U.S. Bank-2.

uu. On or about November 15, 2012, the Subsidiary caused international wire transfers to Stratus Turkey's bank account at Swiss Bank-1, in the amount of approximately \$71,505, which was processed by U.S. Bank-2.

vv. On or about November 15, 2012, the Subsidiary caused an international wire transfer to Stratus Turkey's bank account at Swiss Bank-1, in the amount of approximately \$628,470.60, which was processed by U.S. Bank-2.

ww. On or about December 9, 2012, an individual who was then a high-ranking official at the Stratus Group ("CC-7"), sent a letter to Iranian Government Official-1 requesting, in substance and in part, that Iranian Government Official-1 apply political pressure to the Subsidiary to adhere to the terms of the contract with IIHC.

xx. On or about February 7, 2013, the Subsidiary caused an international wire transfer to Stratus Turkey's bank

account at Swiss Bank-1, in the amount of approximately \$87,141.67, which was processed by U.S. Bank-2.

yy. On or about August 27, 2013, SADR and CC-2 caused a letter to be sent to a representative at the Subsidiary with instructions for the Subsidiary to engage in an international financial transfer to Stratus Turkey for the benefit of IIHC. The letter, which was on IIHC letterhead, requested payment in both USD and Bolivars for IPCs 31 through 37, and provided the following payment instruction details for USD payment: U.S. Bank-2 as the "Intermediary Bank," Swiss Bank-1 as the "Beneficiary's Bank," and Stratus Turkey as the "Beneficiary." For Bolivar payments, the letter listed IIHC as the beneficiary with an account at Venezuelan Bank-1.

zz. On or about November 21, 2013, the Subsidiary caused an international wire transfer to Stratus Turkey's bank account at Swiss Bank-1, in the amount of approximately \$3,140,583.45 for IPCs 31 through 37, which was processed by U.S. Bank-2.

aaa. On or about March 2, 2014, the Project Committee held a meeting, which was attended by SADR, CC-2, and CC-3, among others. During the meeting, the Project Committee, among other things, directed the "Project Management," in substance and in part, to follow up with the Subsidiary to

receive "accumulated monies" for completed activities, which was estimated to be approximately \$10 million USD.

bbb. On or about May 29, 2014, IIHC hosted a Project meeting attended by representatives of IIHC, representatives of the Subsidiary, and Iranian Government Official-1, among others, at which participants discussed IIHC's demands for payment in USD.

(Title 18, United States Code, Section 371).

COUNT TWO

**(Conspiracy to Violate the
International Emergency Economic Powers Act)**

The Grand Jury further charges:

17. The allegations contained in paragraphs 1 through 13 and 16 of this Indictment are repeated and realleged as if fully set forth herein.

18. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to violate, and to cause a violation of, licenses, orders, regulations, and prohibitions issued under the International Emergency Economic

Powers Act, Title 50, United States Code, Sections 1701 to 1707, Part 560 of Title 31, Code of Federal Regulations, and Part 561 of Title 31, Code of Federal Regulations.

19. It was a part and an object of the conspiracy that ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, would and did export, reexport, sell, and supply, and cause to be exported, reexported, sold, and supplied, directly and indirectly, from the United States, services, to wit, international financial transactions, to Iran and to the Government of Iran, without first obtaining the required approval of OFAC, in violation of Title 50, United States Code, Sections 1701 to 1707, and Title 31, Code of Federal Regulations, Section 560.204.

20. It was further a part and an object of the conspiracy that ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, would and did engage in a transaction that evaded and avoided, had the purpose of evading and avoiding, caused a violation of, and attempted to violate one or more of the prohibitions set forth in Title 31, Code of Federal Regulations, Part 560, in violation of Title 50, United States Code, Sections 1701 to 1707, and Title 31, Code of Federal Regulations, Section 560.203.

Overt Acts

21. In furtherance of the conspiracy and to effect the illegal objects thereof, ALI SADR HASHEMI NEJAD, the defendant, and others committed the overt acts set forth in paragraph 16 of this Indictment, which are fully incorporated by reference herein, among others.

(Title 50, United States Code, Section 1705;
Title 31, Code of Federal Regulations, Sections 560.203,
560.204, & 560.205.)

COUNT THREE

(Bank Fraud)

The Grand Jury further charges:

22. The allegations contained in paragraphs 1 through 13 and 16 of this Indictment are repeated and realleged as if fully set forth herein.

23. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, did knowingly execute and attempt to execute a scheme or artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation ("FDIC"), and to obtain moneys, funds, credits, assets, securities, and other property owned by and under the

custody and control of such financial institution, by means of false and fraudulent pretenses, representations, and promises, and aided and abetted the same, to wit, inducing U.S. financial institutions to conduct financial transactions on behalf of and for the benefit of the Government of Iran and Iranian entities and persons using money and property owned by and under the custody and control of such financial institutions, by deceptive means.

(Title 18, United States Code, Sections 1344 & 2.)

COUNT FOUR

(Conspiracy to Commit Bank Fraud)

The Grand Jury further charges:

24. The allegations contained in paragraphs 1 through 13 and 16 of this Indictment are repeated and realleged as if fully set forth herein.

25. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to commit bank fraud, in violation of Title 18, United States Code, Section 1344.

26. It was a part and an object of the conspiracy that ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, would and did knowingly execute and attempt to execute a scheme or artifice to defraud a financial institution, the deposits of which were then insured by the FDIC, and to obtain moneys, funds, credits, assets, securities, and other property owned by and under the custody and control of such a financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

Overt Acts

27. In furtherance of the conspiracy and to effect the illegal object thereof, ALI SADR HASHEMI NEJAD, the defendant, and others committed the overt acts set forth in paragraph 16 of this Indictment, which are fully incorporated by reference herein, among others.

(Title 18, United States Code, Section 1349.)

COUNT FIVE

(Money Laundering)

The Grand Jury further charges:

28. The allegations contained in paragraphs 1 through 13 and 16 of this Indictment are repeated and realleged as if fully set forth herein.

29. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, together with others known and unknown, in an offense involving and affecting interstate and foreign commerce, did knowingly transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds to places in the United States from and through places outside the United States, in amounts exceeding \$10,000, and aided and abetted the same, with the intent to promote the carrying on of specified unlawful activity, to wit, (i) the illegal export of services to Iran as charged in Count Two of this Indictment, and (ii) bank fraud as charged in Counts Three and Four of this Indictment.

(Title 18, United States Code, Sections 1956(a)(2)(A) & 2.)

COUNT SIX

(Conspiracy to Commit Money Laundering)

The Grand Jury further charges:

30. The allegations contained in paragraphs 1 through 13 and 16 of this Indictment are repeated and realleged as if fully set forth herein.

31. From at least in or about 2006, up to and including at least in or about May 2014, in the Southern District of New York, Turkey, Switzerland, Iran, and elsewhere, ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, together with others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to violate Title 18, United States Code, Section 1956(a)(2)(A).

32. It was a part and an object of the conspiracy that ALI SADR HASHEMI NEJAD, the defendant, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds to places in the United States from and through places outside the United States, in amounts exceeding \$10,000, with the intent to promote the carrying on of specified unlawful activity, to wit, the illegal export of services to Iran as charged in Count Two of this Indictment and bank fraud as charged in Counts Three and Four of this Indictment, in violation of Section 1956(a)(2)(A) of Title 18, United States Code.

Overt Acts

33. In furtherance of the conspiracy and to effect the illegal object thereof, ALI SADR HASHEMI NEJAD, the defendant, and others committed the overt acts set forth in paragraph 16 of this Indictment, which are fully incorporated by reference herein, among others.

(Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATIONS

(Counts Two and Three)

34. As a result of committing the offenses alleged in Counts Two and Three of this Indictment, ALI SADR HASHEMI NEJAD, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any and all property constituting or derived from, proceeds obtained directly or indirectly, as a result of the commission of said offenses, including but not limited to (i) a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense that the defendant personally obtained and (ii) all right, title and interest of the defendant in the following specific property: (a) Fresno, California accessor parcel numbers ("APN") 050-040-15s, 050-040-16s, 050-040-17s, 050-190-07s, and 050-220-28s; and (b) 27314 Winding Way, Malibu, CA 90265.

FORFEITURE ALLEGATIONS

(Counts Five and Six)

35. As a result of committing the money laundering offenses alleged in Counts Five and Six of this Indictment, ALI SADR HASHEMI NEJAD, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982, all property, real and personal, involved in the money laundering offenses and all property traceable to such property, including but not limited to, (i) a sum of money representing the amount of property that was involved in the money laundering offense or is traceable to such property and (ii) all right, title and interest of the defendant in the following specific property: (a) Fresno, California APN 050-040-15s, 050-040-16s, 050-040-17s, 050-190-07s, and 050-220-28s; and (b) 27314 Winding Way, Malibu, CA 90265.

Substitute Assets Provision

36. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

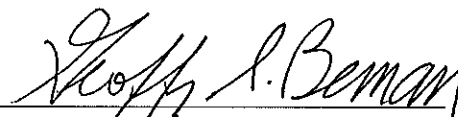
- a) cannot be located upon the exercise of due diligence;
- b) has been transferred or sold to, or deposited with, a third person;
- c) has been placed beyond the jurisdiction of the court;

- d) has been substantially diminished in value;
or
- e) has been commingled with other property
which cannot be subdivided without
difficulty;

it is the intent of the United States, pursuant to Title 21,
United States Code, Section 853(p), to seek forfeiture of any
other property of said defendant up to the value of the above
forfeitable property.

(Title 18, United States Code, Sections 981, 982;
Title 21, United States Code, Section 853;
Title 28, United States Code, Section 2461.)


Foreperson


GEOFFREY S. BERMAN
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

ALI SADR HASHEMI NEJAD,

Defendant.

SEALED INDICTMENT


18 Cr. ____

(18 U.S.C. § 371; 50 U.S.C. § 1705; 31
C.F.R. §§ 560.203, 560.205; 18 U.S.C.
§§ 1349, & 1956.)

GEOFFREY S. BERMAN

United States Attorney.

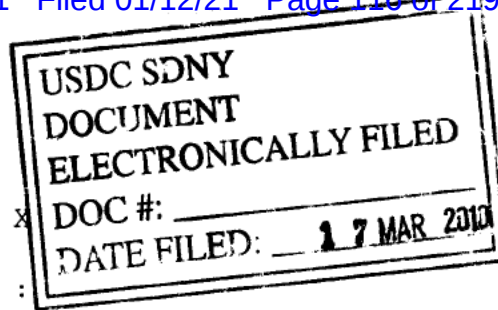
A TRUE BILL



Foreperson.

EXHIBIT K

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK



UNITED STATES OF AMERICA

- v. -

MAHMOUD REZA BANKI,

Defendant.

: SUPERSEDING INDICTMENT

: S1 10 Cr. 08 (JFK)

:

X

COUNT ONE

CONSPIRACY TO VIOLATE IEEPA AND THE ITR AND TO
CONDUCT AN UNLICENSED MONEY TRANSMITTING BUSINESS

The Grand Jury charges:

Background

1. The International Emergency Economic Powers Act, Sections 1701 to 1706 of Title 50 of the United States Code ("IEEPA"), grants to the President of the United States a broad spectrum of powers necessary to "deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat." Title 50, United States Code, Section 1701(a).

2. Pursuant to IEEPA, the President of the United States is authorized, among other things, to "investigate, regulate, or prohibit -- (i) any transactions in foreign exchange, (ii) transfers of credit or payments between, by, through, or to any banking institution, to the extent that such

transfers or payments involve any interest of a foreign country or any national thereof, [and] (iii) the importing and exporting of currency or securities." 50 U.S.C. § 1702(a)(1)(A). Also pursuant to IEEPA, the President is authorized, among other things, to "investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. § 1702(a)(1)(B). The President exercises these IEEPA powers through Executive Orders that impose economic sanctions to address particular emergencies and delegate IEEPA powers for the administration of those sanctions programs.

3. On or about March 15, 1995, President William J. Clinton issued Executive Order 12957, which, among other things, stated that "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and therefore declared "a national emergency to deal with that threat." At all times relevant to this Indictment, Presidents of

the United States have exercised their authority to continue the national emergency declared in Executive Order 12957 through successive presidential notices.

4. On May 6, 1995, the President issued Executive Order 12959, which imposed comprehensive trade and financial sanctions on Iran (the "Iran Trade Embargo"). The Iran Trade Embargo prohibits, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person. The Iran Trade Embargo also prohibits any transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, any prohibition set forth in the Iran Trade Embargo. On August 19, 1997, the President issued Executive Order 13059 consolidating and clarifying the previous orders. The Iran Trade Embargo has been continued and has been in effect at all times relevant to this Indictment. Executive Order 12957, as expanded by Executive Orders 12959 and 13059 (collectively, the "Executive Orders"), was in effect at all times relevant to this Indictment.

5. The Executive Orders authorize the Secretary of the Treasury, in consultation with the Secretary of State, to take such actions, including the promulgation of rules and regulations, as may be necessary to carry out the purposes of the Executive Orders. Pursuant to this authority, the Secretary of

the Treasury promulgated the Iranian Transactions Regulations ("ITR"), 31 C.F.R. Part 560, to implement the sanctions imposed by the Executive Orders. Within the Department of the Treasury, the Office of Foreign Assets Control ("OFAC") is responsible for administering the ITR and adjudicating requests for licenses to engage in transactions otherwise prohibited by the ITR.

6. At all times relevant to this Indictment, the ITR has provided the following:

(i) 31 C.F.R. § 560.201 prohibits the "importation into the United States of any goods or services of Iranian origin or owned or controlled by the Government of Iran, other than information and informational materials."

(ii) 31 C.F.R. § 560.204 prohibits "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran . . . including the exportation, reexportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that: (a) Such goods, technology, or services are intended specifically for supply, transshipment, or reexportation, directly or indirectly, to Iran or the Government of Iran; or (b) Such goods, technology, or services are intended specifically for use in the production of, for commingling with,

or for incorporation into goods, technology, or services to be directly or indirectly supplied, transshipped, or reexported exclusively or predominantly to Iran or the Government of Iran;"

(iii) 31 C.F.R. § 560.203 prohibits "[a]ny transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in [the ITR];"

(iv) 31 C.F.R. § 560.206(a) prohibits a United States person, wherever located, from engaging "in any transaction or dealing in or related to (1) Goods or services of Iranian origin or owned or controlled by the Government of Iran; or (2) Goods, technology, or services for exportation, reexportation, sale, or supply, directly or indirectly, to Iran or the Government of Iran." 31 C.F.R. § 560.206(b) clarifies that "the term transaction or dealing includes but is not limited to purchasing, selling, transporting, swapping, brokering, approving, financing, facilitating, or guaranteeing."

(v) 31 C.F.R. § 560.314 defines a "United States person" as, in relevant part, any United States citizen, permanent resident alien, or any person in the United States.

(vi) Under the ITR, any United States person who wishes to engage in a transaction otherwise prohibited by the ITR

must first file an application for a license and receive approval from OFAC. 31 C.F.R. §§ 560.500, 560.501, and 501.801.

Means And Methods Of the Conspiracy

7. From at least in or about January 2006, up to and including in or about September 2009, MAHMOUD REZA BANKI, the defendant, a citizen of the United States, a resident of Manhattan, New York, and a consultant at a major management consulting firm in Manhattan, provided, among other things, money transmitting services to individuals located in Iran, in violation of the foregoing regulations.

8. More specifically, MAHMOUD REZA BANKI, the defendant, received wire transfers totaling at least approximately \$3.4 million from foreign and domestic companies and individuals into a personal bank account BANKI maintained for this purpose at Bank of America in Manhattan (the "BoFA Account"). The foreign wire originators included companies based in Saudi Arabia, Kuwait, Latvia, Slovenia, Russia, Sweden, and the Philippines. A large portion of the funds wired into the BoFA Account also was transferred to BANKI by Iranian expatriates residing in the United States (the "wire originators"). Generally, BANKI did not know the wire originators personally. BANKI received the funds from the wire originators with the understanding that the funds would, in turn, be disbursed to intended recipients residing in Iran (the "intended recipients").

9. When MAHMOUD REZA BANKI, the defendant, received wire transfers from the wire originators into the BofA Account, he typically would inform an Iran-based co-conspirator not named as a defendant herein ("CC-1") that the funds had been received.

10. Through CC-1 and/or other Iran-based co-conspirators not named as defendants herein, the intended recipients in Iran received the funds, less any fees. The transfers in this case did not involve the physical or electronic transmissions of funds between the United States and Iran. Rather, the conspirators operated an informal value transfer system known as a "hawala." In a hawala system such as the one conducted by MAHMOUD REZA BANKI, the defendant, and his co-conspirators, funds are transferred by customers to a hawala operator, or "hawaladar," in one country (here, the United States), and then corresponding funds, less any fees, are disbursed to recipients in another country (here, Iran) by foreign hawaladars associated with the U.S.-based hawaladar.

11. MAHMOUD REZA BANKI, the defendant, used certain of the funds transferred to the BofA Account by the wire originators to, among other things, purchase a condominium in Manhattan (the "condominium") for approximately \$2.4 million as a joint investment with CC-1; invest in securities for BANKI's own benefit and that of CC-1; and make payments on BANKI's credit card accounts. For example, over an approximately one-month

period in the Summer of 2007, BANKI made credit card payments of approximately \$55,000, drawn from the BofA Account.

12. At all times relevant to this Indictment, MAHMOUD REZA BANKI, the defendant, did not apply for, receive, or possess a license or authorization from OFAC to import from Iran or export to Iran any goods and/or services, or to engage in any transactions or dealings in or related to same.

13. At all times relevant to this Indictment, MAHMOUD REZA BANKI, the defendant, was not licensed to engage in the business of transmitting money by the State of New York.

14. At all times relevant to this Indictment, MAHMOUD REZA BANKI, the defendant, was not registered as a money transmitting business with the United States Treasury Department.

Statutory Allegations

15. From at least in or about January 2006, up to and including in or about September 2009, in the Southern District of New York and elsewhere, MAHMOUD REZA BANKI, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, to violate Sections 1701 to 1706 of Title 50, United States Code, Part 560 of Title 31, Code of Federal Regulations, and Section 1960 of Title 18, United States Code.

16. It was a part and an object of the conspiracy that MAHMOUD REZA BANKI, the defendant, and others known and unknown, unlawfully, willfully, and knowingly would and did conduct financial transactions for the purpose of, and which had the effect of, violating, and which facilitated the violation of, the prohibitions set forth in the Executive Orders and the regulations issued under the International Emergency Economic Powers Act, including the Iranian Transactions Regulations set forth in Title 31, Code of Federal Regulations, Part 560, in violation of Sections 1701 to 1706 of Title 50, United States Code.

17. It was further a part and an object of the conspiracy that MAHMOUD REZA BANKI, the defendant, and others known and unknown, unlawfully, willfully and knowingly would and did conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, BANKI accepted millions of dollars of wire and other transfers into the BofA Account in Manhattan, and, through co-conspirators in Iran, helped to effectuate the transfer of corresponding amounts, less any fees, to residents within Iran, (a) without an appropriate money transmitting license in a State, to wit, New York, where such operation is punishable as a misdemeanor and a felony under State law; (b) while failing to comply with the money transmitting

business registration requirements under Section 5330 of Title 31, United States Code, and regulations prescribed under such section; and (c) knowing that such funds were derived from a criminal offense and were intended to be used to promote and support unlawful activity, to wit, violations of IEEPA and the Executive Orders and regulations attendant thereto, in violation of Section 1960 of Title 18, United States Code.

OVERT ACTS

18. In furtherance of the conspiracy and to effect the illegal objects thereof, MAHMOUD REZA BANKI, the defendant, and others known and unknown, committed the following overt acts in the Southern District of New York and elsewhere:

a. On or about May 10, 2006, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$187,000 into the BofA Account.

b. On or about May 16, 2006, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$60,000 into the BofA Account.

c. On or about August 10, 2006, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$6,000 into the BofA Account.

d. On or about August 12, 2006, MAHMOUD REZA BANKI, the defendant, sent an electronic message to CC-1, in Iran, and

others, confirming, in sum and substance, that BANKI had received \$6,000 into his account.

e. On or about August 14, 2006, a fax was sent from Iran to wire originators residing in the United States, containing instructions necessary to wire transfer funds to the BofA Account of MAHMOUD REZA BANKI, the defendant.

f. On or about August 16, 2006, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$30,000 into the BofA Account.

g. On or about December 6, 2006, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$30,000 into the BofA Account.

h. On or about January 22, 2007, a fax was sent from Iran to wire originators residing in the United States, containing instructions necessary to wire transfer funds to the BofA Account of MAHMOUD REZA BANKI, the defendant.

i. On or about January 22, 2007, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of approximately \$100,000 into the BofA Account.

j. On or about November 5, 2007, MAHMOUD REZA BANKI, the defendant, received a wire transfer in the amount of

approximately \$75,000 into the BofA Account.

(Title 50, United States Code, Section 1705;
Title 18, United States Code, Section 371.)

COUNT TWO
VIOLATION OF IEEPA AND THE ITR

The Grand Jury further charges:

19. The allegations set forth in paragraphs 1 through 14 are repeated and realleged as if set forth fully herein.

20. From at least in or about January 2006 through at least in or about September 2009, MAHMOUD REZA BANKI, the defendant, unlawfully, willfully, and knowingly conducted financial transactions for the purpose of, and which had the effect of, violating, and which facilitated the violation of, the prohibitions set forth in the Executive Orders and the regulations issued under the International Emergency Economic Powers Act, including the Iranian Transactions Regulations set forth in Title 31, Code of Federal Regulations, Part 560, to wit, BANKI provided money transfer services, through the operation of a "hawala" informal value transfer system, to persons in Iran.

(Title 50, United States Code, Sections 1701 to 1706, and
Title 18, United States Code, Section 2.)

COUNT THREE
CONDUCTING AN UNLICENSED
MONEY TRANSMITTING BUSINESS

The Grand Jury further charges:

21. The allegations set forth in paragraphs 1 through 14 are repeated and realleged as if set forth fully herein.

22. From at least in or about January 2006 through at least in or about September 2009, in the Southern District of New York and elsewhere, MAHMOUD REZA BANKI, the defendant, unlawfully, willfully and knowingly, conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, BANKI accepted millions of dollars of wire and other transfers into the BofA Account in Manhattan, and subsequently effectuated, and aided and abetted, the transfer of corresponding amounts, less any fees, to residents within Iran, (a) without an appropriate money transmitting license in a State, to wit, New York, where such operation is punishable as a misdemeanor and a felony under State law; (b) while failing to comply with the money transmitting business registration requirements under Section 5330 of Title 31, United States Code, and regulations prescribed under such section; and © knowing that such funds were derived from a criminal offense and were intended to be used to promote and support unlawful activity, to wit,

violations of IEEPA and the Executive Orders and regulations attendant thereto.

(Title 18, United States Code, Sections 1960 and 2.)

COUNT FOUR

FALSE STATEMENTS

The Grand Jury further charges:

23. The allegations set forth in paragraphs 1 through 14 are repeated and realleged as if set forth fully herein.

24. On or about January 16, 2008, in the Southern District of New York and elsewhere, MAHMOUD REZA BANKI, the defendant, unlawfully, willfully, and knowingly, in a matter within the jurisdiction of the executive branch of the Government of the United States, did falsify, conceal and cover up by trick, scheme, and device, material facts and did make materially false, fictitious, and fraudulent statements and representations, to wit, in response to a written request by OFAC that BANKI provide "detailed information" regarding a January 22, 2007 transfer of \$100,000 to his BofA Account, including "an explanation of the purpose of the payment, the names, addresses and any other information available on the parties involved in the transaction and a description of the relationships between those parties," which request advised BANKI that "under U.S. Criminal Code (Title 18, Section 1001), knowingly falsifying or concealing a material

fact in your response to this letter is a felony," which may result in fines and/or imprisonment, or both, BANKI stated to OFAC in writing, among other things, that "[t]he payment in question was a gift from the extended family" and that "[t]he payment originally came from one of these family members: 'Ali Alaie' who is an Iranian citizen and resides in Tehran, Iran," whereas, in truth and in fact, the aforementioned payment originated from BANKI's father, a United States citizen.

(Title 18, United States Code, Section 1001(a).)

COUNT FIVE
FALSE STATEMENTS

The Grand Jury further charges:

25. The allegations set forth in paragraphs 1 through 14 are repeated and realleged as if set forth fully herein.

26. On or about July 31, 2008, in the Southern District of New York and elsewhere, MAHMOUD REZA BANKI, the defendant, unlawfully, willfully, and knowingly, in a matter within the jurisdiction of the executive branch of the Government of the United States, did falsify, conceal and cover up by trick, scheme, and device, material facts and did make materially false, fictitious, and fraudulent statements and representations, to wit, in response to a written request by OFAC that BANKI detail "all payments [he had] made, received, or facilitated in any

manner involving Iran since July 1, 2003," which request advised BANKI that "under U.S. Criminal Code (Title 18, Section 1001), knowingly falsifying or concealing a material fact in your response to this letter is a felony," which may result in fines and/or imprisonment, or both, BANKI stated to OFAC in writing, among other things, that "[m]y first cousin Ali Alaie kindly offered to provide the funds for me to purchase my New York real estate"; that all transfers to BANKI's BofA account during the period November 20, 2006 through January 16, 2007 were "sent by Mr. Ali Alaie to my bank account by wire transfers"; and that BANKI had "not facilitated in any manner payments involving Iran," whereas, in truth and in fact, the aforementioned payments originated from BANKI's father, a United States citizen, and BANKI had knowingly facilitated the transfer of funds to Iran from the United States through the use of his BofA account.

(Title 18, United States Code, Section 1001(a).)

FORFEITURE ALLEGATIONS AS TO COUNTS ONE AND TWO

27. As the result of committing the offenses in violation of Title 18, United States Code, Section 371 and Title 50, United States Code, Section 1705, alleged in Counts One and Two of this Indictment, MAHMOUD REZA BANKI, the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)© and 28 U.S.C. § 2461, all property, real and personal, that

constitutes or is derived from proceeds traceable to the commission of the offense, including but not limited to the following:

a. At least \$3,400,000 in United States currency, in that such sum in aggregate is property representing the amount of proceeds obtained as a result of the offenses.

b. All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 135 West 4th Street, Unit #1W, New York, New York, 10012, more particularly described as: Lot 1201 and Block 552.

c. All United States currency funds or other monetary instruments credited to account numbers 0042 0105 0158, 910 000 7976 4616, 910 000 8269 7686, 910 000 8269 7712, 910 000 8596 8587, 910 000 8596 8626, 910 000 9235 4676, 910 000 9379 7423, 910 000 9379 7449, 910 000 9379 7465, 3810 0804 1874, and 910 001 0212 1870, in the name of Mahmoud Banki, located at Bank of America.

d. All United States currency funds or other monetary instruments credited to account number EBH-210390, in the name of Mahmoud R. Banki, located at Chase Investment Services Corp.

e. All United States currency funds or other monetary instruments credited to account number Z72-275735, in the name of Mahmoud Banki, located at Fidelity Investments.

f. All United States currency funds or other monetary instruments credited to account numbers 849-11383, 849-15041, and 849-11493, in the name of Mahmoud Banki, located at Merrill Lynch.

Substitute Asset Provision

28. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(1) cannot be located upon the exercise of due diligence;

(2) has been transferred or sold to, or deposited with, a third person;

(3) has been placed beyond the jurisdiction of the Court;

(4) has been substantially diminished in value; or

(5) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 371 and 981;
Title 28, United States Code, Section 2461;
Title 50, United States Code, Section 1705.)

FORFEITURE ALLEGATIONS AS TO COUNT THREE

29. As the result of committing the offense in violation of 18 U.S.C. § 1960, alleged in Count Three of this Indictment, MAHMOUD REZA BANKI, the defendant, shall forfeit to the United States pursuant to 18 U.S.C. § 982, all property, real and personal, involved in the offense and all property traceable to such property, including but not limited to the following:

a. At least \$3,400,000 in United States currency, in that such sum in aggregate is property representing the amount of proceeds obtained as a result of the offenses.

b. All that lot or parcel of land, together with its buildings, appurtenances, improvements, fixtures, attachments and easements, located at 135 West 4th Street, Unit #1W, New York, New York, 10012, more particularly described as: Lot 1201 and Block 552.

c. All United States currency funds or other monetary instruments credited to account numbers 0042 0105 0158, 910 000 7976 4616, 910 000 8269 7686, 910 000 8269 7712, 910 000 8596 8587, 910 000 8596 8626, 910 000 9235 4676, 910 000 9379 7423, 910 000 9379 7449, 910 000 9379 7465, 3810 0804 1874, and 910 001

0212 1870, in the name of Mahmoud Banki, located at Bank of America.

d. All United States currency funds or other monetary instruments credited to account number EBH-210390, in the name of Mahmoud R. Banki, located at Chase Investment Services Corp.

e. All United States currency funds or other monetary instruments credited to account number Z72-275735, in the name of Mahmoud Banki, located at Fidelity Investments.

f. All United States currency funds or other monetary instruments credited to account numbers 849-11383, 849-15041, and 849-11493, in the name of Mahmoud Banki, located at Merrill Lynch.

Substitute Asset Provision

30. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(1) cannot be located upon the exercise of due diligence;

(2) has been transferred or sold to, or deposited with, a third person;

(3) has been placed beyond the jurisdiction of the Court;

(4) has been substantially diminished in value; or

(3) has been placed beyond the jurisdiction of the Court;

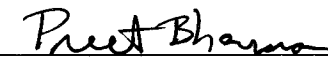
(4) has been substantially diminished in value; or

(5) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982 and 1960.)


FOREPERSON


PREET BHARARA
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA

- v. -

MAHMOUD REZA BANKI,

Defendant.

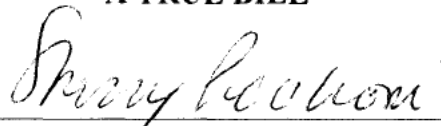
SUPERSEDING INDICTMENT

(Title 18, United States Code, Sections 2, 371, 1960, 1001,
Title 50, United States Code, Sections 1701 to 1706.)

PREET BHARARA

United States Attorney.

A TRUE BILL



Foreperson.

3/17/10 Superseding indictment filed.

Pitman, U.S.M.J.

EXHIBIT L

[REDACTED]

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

- against -

HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA INC.,
FUTUREWEI TECHNOLOGIES, INC.,
SKYCOM TECH CO., LTD.,
WANZHOU MENG,
also known as “Cathy Meng” and
“Sabrina Meng,”

[REDACTED]

S U P E R S E D I N G
I N D I C T M E N T

Cr. No. 18-457 (S-3) (AMD)
(T. 18, U.S.C., §§ 371, 981(a)(1)(C),
982(a)(1), 982(a)(2), 982(b)(1), 1343,
1344, 1349, 1512(k), 1832(a)(5),
1832(b), 1956(h), 1962(d), 1963(a),
1963(m), 2323(b)(1), 2323(b)(2), 2 and
3551 et seq.; T. 21, U.S.C., § 853(p);
T. 28, U.S.C., § 2461(c); T. 50, U.S.C.,
§§ 1702, 1705(a) and 1705(c))

Defendants.

----- X

THE GRAND JURY CHARGES:

I N T R O D U C T I O N

At all times relevant to this Superseding Indictment, unless otherwise
indicated:

I. The Defendants

1. The defendant HUAWEI TECHNOLOGIES CO., LTD. (“HUAWEI”) was a global networking, telecommunications and services company headquartered in Shenzhen, Guangdong, in the People’s Republic of China (“PRC”). As of the date of the filing of this Superseding Indictment, HUAWEI was the largest telecommunications

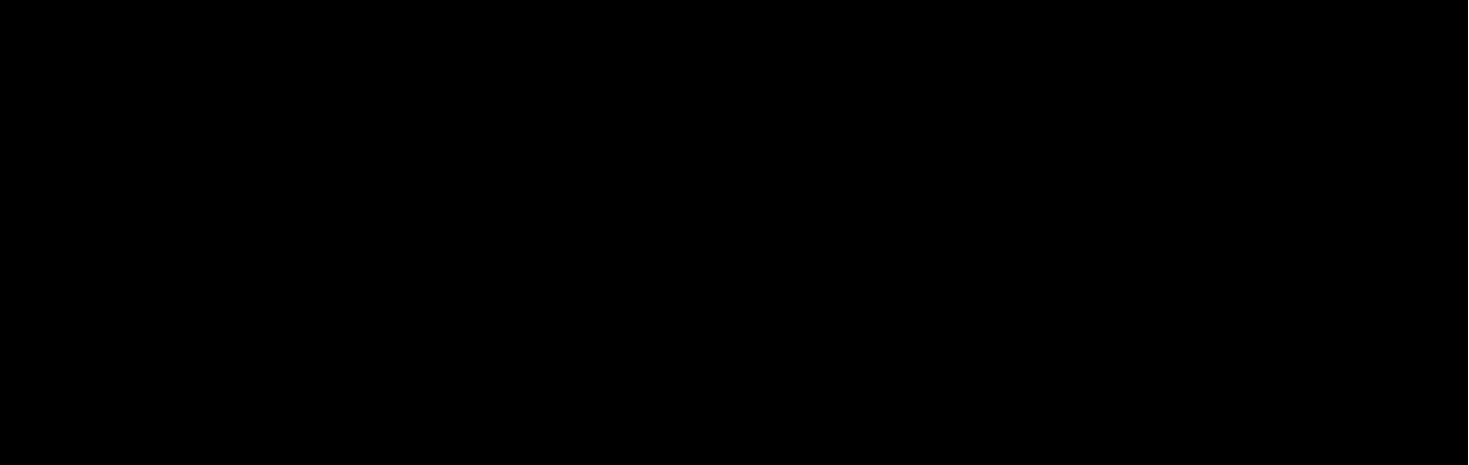
equipment manufacturer in the world. HUAWEI was owned by its parent company, Huawei Investment & Holdings Co., Ltd. (“Huawei Holdings”), which was registered in Shenzhen, Guangdong, PRC, and predecessor entities of that company.

2. The defendant HUAWEI DEVICE CO., LTD. (“HUAWEI DEVICE”) was a company in the PRC that designed and manufactured wireless phones. HUAWEI DEVICE was a subsidiary of HUAWEI.

3. The defendant HUAWEI DEVICE USA INC. (“HUAWEI DEVICE USA”), a manufacturer of communication products whose headquarters was in the United States, and the defendant FUTUREWEI TECHNOLOGIES, INC. (“FUTUREWEI”), a research and development company whose headquarters was in the United States, were both subsidiaries of HUAWEI and Huawei Holdings.

4. The defendant SKYCOM TECH CO., LTD. (“SKYCOM”) was a corporation registered in Hong Kong whose primary operations were in Iran. SKYCOM functioned as HUAWEI’s Iran-based subsidiary. As of 2007, Huawei Holdings owned SKYCOM through a subsidiary (“Huawei Subsidiary 1”), an entity the identity of which is known to the Grand Jury. In or about November 2007, Huawei Subsidiary 1 transferred its shares of SKYCOM to another entity (“Huawei Subsidiary 2”), an entity the identity of which is known to the Grand Jury, which was purportedly a third party in the transaction but was actually controlled by HUAWEI. Following this transfer of SKYCOM shares from Huawei Subsidiary 1 to Huawei Subsidiary 2, HUAWEI falsely claimed that SKYCOM was one of HUAWEI’s local business partners in Iran, as opposed to one of HUAWEI’s subsidiaries or affiliates.

5. The defendant WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” was a citizen of the PRC. From at least in or about 2010, MENG served as Chief Financial Officer of HUAWEI. Between approximately February 2008 and April 2009, MENG served on the SKYCOM Board of Directors. More recently, MENG also served as Deputy Chairwoman of the Board of Directors for HUAWEI.



II. The Scheme to Misappropriate Intellectual Property

8. Since at least in or about 2000 through the date of this Superseding Indictment, the defendants HUAWEI, FUTUREWEI, HUAWEI DEVICE and HUAWEI DEVICE USA (the “IP Defendants”) and others executed a scheme to operate and grow the worldwide business of HUAWEI and its parents, global affiliates and subsidiaries through the deliberate and repeated misappropriation of intellectual property of companies headquartered or with offices in the United States (the “Victim Companies”) for commercial use. By misappropriating the intellectual property of the Victim Companies, the IP Defendants received income directly and indirectly, including by benefitting from the sale of products containing stolen intellectual property and saving on research and development costs, which income the IP Defendants agreed to use to establish and operate the worldwide

business of Huawei and its parents, global affiliates and subsidiaries, including in the United States.

9. The misappropriated intellectual property of the Victim Companies comprised or included trade secret information, as defined by Title 18, United States Code, Section 1839(3), and other confidential and nonpublic intellectual property. To protect trade secret information and other intellectual property from disclosure, the Victim Companies each employed reasonable measures, including but not limited to physical, electronic and network security, company policy and training, and legal agreements and contracts. The IP Defendants believed that the misappropriated intellectual property comprised or contained trade secret information, and knew and intended that such misappropriation would injure the Victim Companies.

10. The misappropriated intellectual property of Victim Companies consisted of 10 or more copies of copyrighted works with a value greater than \$2,500 within a period of 180 days, as defined and described within Title 18, United States Code, Section 2319. The IP Defendants knew and intended that the misappropriation of copyrighted works would injure the Victim Companies.

11. To obtain the intellectual property of the Victim Companies, the IP Defendants sometimes entered into confidentiality agreements with the owners of the intellectual property and then violated the terms of the confidentiality agreements by misappropriating the intellectual property for the IP Defendants' own commercial use. The IP Defendants also tried to recruit employees of the Victim Companies in order to gain access to intellectual property of their former employers, and the IP Defendants directed and incentivized their own employees to steal intellectual property from other companies.

12. On other occasions, the IP Defendants used proxies such as professors working at research institutions or third party companies, purporting not to be working on behalf of the IP Defendants, to gain access to the Victim Companies' nonpublic intellectual property. Those proxies then impermissibly provided the Victim Companies' nonpublic proprietary information to the IP Defendants.

13. In another effort to gain access to the nonpublic intellectual property of the Victim Companies, in 2013, HUAWEI launched a formal policy instituting a bonus program to reward employees who obtained confidential information from competitors. Under the policy, HUAWEI established a formal rewards schedule to pay employees of HUAWEI affiliates for stealing information from competitors based upon the value of the information obtained. Employees were directed to post confidential information obtained from other companies on an internal HUAWEI website, or, in the case of especially sensitive information, to send an encrypted email to a special huawei.com email mailbox. A "competition management group" was tasked with reviewing the submissions and awarding monthly bonuses to the employees who provided the most valuable stolen information. Biannual awards also were made available to the top "Huawei Regional Divisions" that provided the most valuable information. A memorandum describing this program was sent to employees in the United States.

14. To avoid and minimize the costs of potential civil and criminal liability in the United States, and therefore more easily establish and operate HUAWEI's U.S. business, the IP Defendants engaged in a pattern of obstruction. In advance of and during civil proceedings regarding the IP Defendants' alleged misappropriation of intellectual property, the IP Defendants provided false information in the form of affidavits or reports of

internal investigations, to minimize potential liability for the misappropriation of intellectual property. Similarly, the IP Defendants instructed employees to conceal information from law enforcement. For example, an official HUAWEI manual labeled “Top Secret” instructed certain individuals working for HUAWEI to conceal their employment with HUAWEI during encounters with foreign law enforcement officials.

15. To prevent civil and criminal liability, as well as reputational harm, when confronted with evidence of their wrongdoing, the IP Defendants publicly blamed the wrongdoing on purportedly rogue low-level employees of HUAWEI and its subsidiaries and affiliates.

16. HUAWEI, HUAWEI DEVICE USA and FUTUREWEI agreed to use the proceeds derived from the theft of intellectual property to establish and operate the business of HUAWEI and its parents, global affiliates and subsidiaries in the United States and abroad. Similarly, HUAWEI, HUAWEI DEVICE USA and FUTUREWEI agreed to benefit from cost savings generated by stolen intellectual property to innovate more quickly and thus to also establish and operate the business of HUAWEI and its parents, and global affiliates and subsidiaries in the United States and abroad.

17. As part of the scheme to establish and operate the business of HUAWEI and its parents, global affiliates and subsidiaries in the United States and elsewhere, and to avoid interference in their scheme by U.S. governmental bodies or other private actors, HUAWEI, HUAWEI DEVICE USA and FUTUREWEI repeatedly made material misrepresentations as to the misappropriation and subsequent commercial use of intellectual property, as well as other criminal activity, including the nature and extent of business in high-risk jurisdictions such as Iran, to U.S. governmental bodies from whom

HUAWEI, HUAWEI DEVICE USA and FUTUREWEI sought regulatory authorization that would help grow the IP Defendants' U.S.-based business. HUAWEI, HUAWEI DEVICE USA and FUTUREWEI made similar material misrepresentations to financial institutions from whom the defendants sought banking services.

A. Company 1

18. Beginning in or about 2000, the defendants HUAWEI and FUTUREWEI misappropriated operating system source code for internet routers, command line interface (a structure of textual commands used to communicate with routers) and operating system manuals from a U.S. technology company headquartered in the Northern District of California ("Company 1"), an entity the identity of which is known to the Grand Jury, and incorporated the misappropriated source code into HUAWEI internet routers that FUTUREWEI sold in the United States from approximately April 2002 until December 2002. Toward this end, HUAWEI and FUTUREWEI hired or attempted to hire Company 1 employees and directed these employees to misappropriate Company 1 source code on behalf of the defendants. Company 1 had registered as copyrighted the material misappropriated by HUAWEI and FUTUREWEI.

19. HUAWEI and FUTUREWEI publicly marketed their internet routers in the United States as lower cost versions of Company 1 internet routers; HUAWEI and FUTUREWEI's routers featured model numbers, user interfaces and operating manuals similar to those of routers sold by Company 1. In actuality, HUAWEI and FUTUREWEI's internet routers were essentially direct copies of routers sold by Company 1.

20. In or about December 2002, representatives of Company 1 notified senior HUAWEI executives, including the founder of HUAWEI ("Individual-1"), an

individual whose identity is known to the Grand Jury, of the misappropriation. After approximately one month of negotiation, the defendants HUAWEI and FUTUREWEI agreed to replace the original versions of some of the misappropriated source code and to recall from the U.S. market products that included misappropriated source code.

21. In or about 2003, Company 1 filed suit against the defendants HUAWEI and FUTUREWEI in federal court in the Eastern District of Texas for infringement of intellectual property. At the outset of the litigation, HUAWEI and FUTUREWEI claimed to have already removed Company 1's source code from products and recalled routers containing any stolen source code in early 2003. However, as part of this recall effort and to obstruct the civil litigation, HUAWEI and FUTUREWEI erased the memory drives of recalled HUAWEI routers and then sent those routers to the PRC before Company 1 could access them, thus destroying evidence of HUAWEI and FUTUREWEI's illicit conduct. Also, in an effort to destroy evidence, FUTUREWEI attempted to remotely access HUAWEI routers that had already been sold in the United States and erase the misappropriated source code contained therein.

22. In the litigation against Company 1, a HUAWEI executive vice president, an individual whose identity is known to the Grand Jury, filed a declaration on behalf of the defendants HUAWEI and FUTUREWEI falsely claiming that the defendants had received Company 1's source code from a third party. HUAWEI and FUTUREWEI submitted this false declaration to minimize potential civil damages in the pending litigation by making it appear that HUAWEI had not knowingly misappropriated Company 1's source code but rather benefitted from a munificent third party.

23. As part of the litigation, the parties agreed that a neutral expert would examine the source code used by Company 1 and HUAWEI in internet routers from which HUAWEI and FUTUREWEI had purportedly removed copied source code. In a limited examination of small portions of the source code at issue, the neutral expert found that source code for two sequences of HUAWEI program instructions (“routines”) were substantially similar to or developed or derived from Company 1’s source code: “It is clear that there was Substantial Similarity in portions of the Huawei . . . code and that there has been copyright infringement.” In particular, the neutral expert found “the conclusion is unescapable” that one routine of HUAWEI source code is “Substantially Similar to [Company 1]’s [source code] and has been misappropriated.” With respect to four other programming routines, the neutral expert agreed with Company 1 that portions of those routines “were copied from [Company 1] source code,” and one routine “was copied in its entirety and modified slightly.”

24. From approximately April 2002 until December 2002, FUTUREWEI sold HUAWEI routers containing Company 1’s source code in the United States. The efforts by FUTUREWEI and HUAWEI to obstruct civil litigation with Company 1, including by filing a declaration with false information and destroying evidence of misappropriation, were designed to save costs from litigation and avoid possible regulatory or law enforcement action.

B. Company 2

25. In or about and between 2000 and 2003, an engineer (“Engineer-1”), an individual whose identity is known to the Grand Jury, engaged in efforts to misappropriate the intellectual property of a U.S. technology company headquartered in the Northern

District of Illinois (“Company 2”), an entity the identity of which is known to the Grand Jury, and provide the intellectual property to HUAWEI. Engineer-1 was employed by Company 2.

26. No later than October 2001, HUAWEI had identified Engineer-1 as a target for recruitment in light of his employment with Company 2. In an October 9, 2001 email, which subject read “[Company 2] [Engineer-1] visit in Huawei,” a HUAWEI employee wrote that Engineer-1 worked for Company 2, and that:

[He] has more than 40 patents. Last year, when [Engineer-1] had a meeting with [Individual-1] and [Huawei’s Chief Strategy Marketing Officer (“Individual-2”, an individual whose identity is known to the Grand Jury)] in Huawei, [Individual-1] asked [Engineer-1] to join Huawei. Considering his team members (more than 10 people), he refused the proposal. Now he is coming to seek opportunity to cooperate with Huawei in a few products. He will come to China around October 20 and wishes to meet Individual-2 and Huawei people from relevant business departments.

The recipient of the email responded, “At present, we can communicate with him to see whether he has any primary plan or proposal for cooperation and cooperation in what products.” As part of this recruitment effort, between in or about 2000 and 2003, Engineer-1 met personally with Individual-1 and other HUAWEI executives multiple times in the PRC.

27. For example, in or about February 2003, Engineer-1 met with Individual-1 in the PRC. On or about March 3, 2003, Engineer-1 wrote an email to Individual-1 and another HUAWEI employee stating, “Attached please find those document [sic] about [Company 2 base station technology] specification you asked.” The email attached a 50-page document with technical specifications for a base station, designed for use

in wireless network, manufactured by Company 2. Each page of the document bore the marking “[Company 2] Confidential Property.” The cover page of the document stated, “This document and the information contained in it is Confidential Information of [Company 2] and shall not be used, published[,] disclosed, or disseminated outside of [Company 2].”

C. Company 3

28. In or about July 2004, at a trade show in Chicago, Illinois, a HUAWEI employee (“Individual-3”), an individual whose identity is known to the Grand Jury, was discovered in the middle of the night after the show had closed for the day in the booth of a technology company (“Company 3”), an entity the identity of which is known to the Grand Jury, removing the cover from a networking device and taking photographs of the circuitry inside. Individual-3 wore a badge listing his employer as “Weihua,” HUAWEI spelled with its syllables reversed. In official correspondence with Company 3 shortly after this incident, HUAWEI claimed that Individual-3 attended the trade show in his personal capacity and that his attempted misappropriation occurred “without Huawei’s authorization.” According to a purported official statement published in Reuters, HUAWEI claimed, “This is a junior engineer who had never traveled to the United States before. His actions do not reflect the culture or values of Huawei.” Notably, a resume that Individual-3 submitted to the U.S. government in approximately 2012 stated that he had been a “senior R&D Engineer” at HUAWEI from 1997 until July 2004, the time of the incident.

29. The efforts to misappropriate the intellectual property of Company 3 were designed to permit HUAWEI to save on research and development costs in the development of its own networking device.

D. Company 4

30. In or about 2009, HUAWEI and FUTUREWEI devised a scheme to misappropriate technology related to antennas that provide cellular telephone and data services. The technology was developed by a technology company operating in the Northern District of California and the Western District of New York (“Company 4”), an entity the identity of which is known to the Grand Jury.

31. In or about September 2009, FUTUREWEI entered into a non-disclosure agreement (“NDA”) with Company 4, which prevented FUTUREWEI from using confidential information provided by Company 4 for FUTUREWEI’s own benefit or to the competitive disadvantage of Company 4.

32. On or about September 21, 2009, Company 4 provided a presentation to HUAWEI and FUTUREWEI regarding Company 4’s proprietary technology to improve reception between cellular telephones and the antennas that provide cellular telephone and data services, which was a trade secret of Company 4. Each slide was marked “Commercial In Confidence.” Thereafter, in response to questions from a FUTUREWEI engineer (“Engineer-2”), Company 4 provided additional information regarding the technology.

33. While expressing outward enthusiasm for a potential partnership with Company 4, HUAWEI and FUTUREWEI secretly worked to misappropriate the Company 4 technology provided pursuant to the NDA. On or about September 21, 2009, the same day that Company 4 provided the presentation to HUAWEI and FUTUREWEI, a HUAWEI employee wrote an email to Engineer-2 at FUTUREWEI expressing interest in the technology on which Company 4 had presented. On or about October 23 and October 26, 2009, Engineer-2 wrote two emails to his colleagues indicating that he was very interested in

the Company 4 technology and had some ideas on how to implement the technology. On or about October 30, 2009, FUTUREWEI filed a provisional patent application with the U.S. Patent and Trademark Office that used and relied in large part upon the Company 4 intellectual property.

34. In or about and between approximately 2009 and 2016, HUAWEI received approximately \$22 million in income derived from the sale of products that incorporated intellectual property misappropriated from Company 4.

E. Company 5

35. In or about 2012 and 2013, HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA devised a scheme to misappropriate robot technology from a U.S. wireless network operator headquartered in the Western District of Washington (“Company 5”), an entity the identity of which is known to the Grand Jury. In May 2012, HUAWEI DEVICE USA asked Company 5 to sell or license its proprietary robotic system for testing phones to HUAWEI DEVICE USA; Company 5 declined. Thereafter, HUAWEI and HUAWEI DEVICE began to develop their own robotic phone-testing system, and directed HUAWEI DEVICE USA employees to provide detailed information about Company 5’s technology to support that effort.

36. Beginning in or about August 2012, HUAWEI DEVICE USA and Company 5 executed a series of confidentiality agreements allowing select HUAWEI DEVICE USA employees access to a Company 5 robot laboratory. HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA employees abused this restricted access in order to misappropriate Company 5 technology. In a November 6, 2012 email, a HUAWEI engineer directed a HUAWEI DEVICE USA employee, “[T]his email is just a kindly reminder for the

information we need to build our own robot system and kindly feedback the information we need in the attachment . . .” Attached to the email was a file requesting information about the technical specifications of the robot hardware components and software systems. The HUAWEI DEVICE USA employee responded, “[HUAWEI DEVICE USA engineers] have accessed the [Company 5] robot lab They know how [Company 5] robot work and system info. I asked them to write down the info in detail and then send to [HUAWEI and HUAWEI DEVICE].”

37. In or about and between November 2012 and January 2013, in response to technical questions from HUAWEI and HUAWEI DEVICE, HUAWEI DEVICE USA employees sent HUAWEI and HUAWEI DEVICE multiple photographs of the Company 5 robot and its software interface system taken from inside the secure Company 5 laboratory, in violation of the confidentiality agreements. In or about January 2013, HUAWEI DEVICE USA suggested that HUAWEI and HUAWEI DEVICE send their own engineer to Company 5’s laboratory in Seattle, Washington: “You will learn a lot in knowledge and experience.” In or about and between March and April 2013, HUAWEI and HUAWEI DEVICE continued to develop their own robot while directing HUAWEI DEVICE USA employees to provide more information about Company 5’s robot.

38. In or about May 2013, HUAWEI sent an engineer working on the robot project (“Engineer-3”), an individual whose identity is known to the Grand Jury, to the United States. Engineer-3 wrote to HUAWEI DEVICE USA, describing his trip as follows: “go to the [Company 5] laboratory for reconnaissance and obtain measurement data.”

39. On or about and between May 13 and 14, 2013, HUAWEI DEVICE USA employees allowed to access the Company 5 laboratory improperly used their badges to

allow Engineer-3 access. Once inside, Engineer-3 photographed and gathered technical information about the robot before Company 5 personnel discovered the breach and escorted him out of the facility. Engineer-3 then emailed HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA personnel the photographs and technical information he had improperly gathered.

40. On or about May 29, 2013, a HUAWEI DEVICE USA employee accessed the laboratory and surreptitiously placed a robot arm into a laptop bag and removed the robot arm from the laboratory. Before the robot arm was returned to Company 5—which had discovered the theft—Engineer-3 took measurements of the robot arm and emailed photographs and measurements to HUAWEI and HUAWEI DEVICE engineers.

41. On or about August 13, 2013, HUAWEI DEVICE USA issued an “Investigation Report,” which purported to summarize the findings of an internal investigation into the above-described misconduct in the Company 5 robot laboratory. HUAWEI DEVICE USA subsequently provided a copy of the report to Company 5. The report falsely described the actions of Engineer-3 and HUAWEI DEVICE USA in May 2013 as “isolated incidents,” and characterized Engineer-3’s actions as a “moment of indiscretion.” Additionally, a HUAWEI DEVICE USA employee falsely informed Company 5 that there were “not a lot of emails” discussing the Company 5 robot, when, in fact, there was extensive email correspondence among HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA in which HUAWEI and HUAWEI DEVICE employees directed HUAWEI DEVICE USA employees to misappropriate information from Company 5.

42. On or about May 19, 2014, HUAWEI sent a letter to Company 5 describing disciplinary measures taken in response to the actions of Engineer-3 and

HUAWEI DEVICE USA, and claiming that HUAWEI did not condone those actions and that respect for intellectual property rights was one of HUAWEI's "core principles."

43. Company 5 ultimately filed a civil lawsuit against HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA.

44. The efforts to misappropriate the intellectual property of Company 5 were designed to permit HUAWEI DEVICE to save on research and development costs in the development of its own testing robot for use on HUAWEI DEVICE prototypes. The efforts to obstruct civil litigation with Company 5, such as misstatements regarding the quantity of relevant email correspondence, were designed to save litigation costs and to avoid scrutiny by regulators and law enforcement.

F. Company 6

45. In or about and between 2013 and 2018, HUAWEI devised a scheme to misappropriate technology from a U.S. developer of architecture for memory hardware headquartered in the Northern District of California ("Company 6"), an entity the identity of which is known to the Grand Jury.

46. Not long after the corporate formation of Company 6—which was a direct competitor of HUAWEI in the field of memory hardware architectural design—HUAWEI devised a corporate strategy to misappropriate proprietary technology from Company 6. An internal HUAWEI presentation from in or about 2015 articulated the "countermeasures" planned against Company 6, including "continuously recruit[ing] people from [Company 6]" in order to cause "internal turmoil" at Company 6. The same document included an organizational chart for Company 6, listing the names and compensation information for Company 6 employees located both in the United States and in the PRC.

47. As part of its scheme to misappropriate Company 6's technology, HUAWEI invited principals of Company 6 to make a presentation in Shenzhen, PRC in or around June 2015 about Company 6's technology regarding architecture for solid state drives, a kind of data storage device. After the presentation, HUAWEI sought a copy of the slide deck that Company 6 had used in its presentation; in the course of these communications, HUAWEI falsely expressed interest in developing a commercial relationship with Company 6. After receiving HUAWEI's oral promises that it would maintain the confidentiality of the information contained in the slide deck, including that HUAWEI would not share this information with HUAWEI's subsidiary that at the time was developing competing technology, Company 6 sent a copy of the slide deck to HUAWEI. Immediately upon receipt of the slide deck, each page of which was marked "Proprietary and Confidential" by Company 6, HUAWEI distributed the slide deck to HUAWEI engineers, including engineers in the subsidiary that was working on technology that directly competed with Company 6's products and services. These engineers discussed developments by Company 6 that would have application to HUAWEI's own prototypes then under design. Such actions were inconsistent with HUAWEI's previously stated intent to develop a commercial relationship with Company 6.

48. Acting at the direction of the Rotating Chairman of HUAWEI, a HUAWEI engineer ("Engineer-4"), an individual whose identity is known to the Grand Jury, visited Company 6's headquarters in the Northern District of California during the summer of 2016. According to a message sent to Company 6, Engineer-4 sought the meeting because "We are choosing . . . your company or [a competitor] to develop the [solid state drive] disc for our next generation of hard discs." After a meeting with a principal of

Company 6, an individual whose identity is known to the Grand Jury, where the principal provided an oral overview of Company 6's plans for architectural design, Engineer-4 wrote an internal HUAWEI email attaching a slide presentation detailing some of Company 6's intellectual property. The email stated, "Our idea of [solid state drive] and controller coordination is good but we acted a bit late."

49. HUAWEI did not follow up on Engineer-4's representations to Company 6 that HUAWEI intended to consider purchasing Company 6's products or services. Rather, HUAWEI made efforts to obtain Company 6's nonpublic technology without directly engaging Company 6. For example, two HUAWEI employees, individuals whose identities are known to the Grand Jury, including a principal of HUAWEI's chip design team, wrote to Company 6's generic email address, without concealing their affiliation with HUAWEI, requesting samples of Company 6's products, which were not then publicly available. Company 6 did not respond to these email requests, which were considered unusual business practice and possible efforts to misappropriate Company 6's protected intellectual property.

50. HUAWEI used a proxy to obtain information about Company 6's proprietary technology. Specifically, a professor of a PRC research university (the "Professor"), an individual whose identity is known to the Grand Jury, gained access to Company 6's proprietary technology on HUAWEI's behalf. An internal HUAWEI document from in or about early 2017 detailed the need to use such proxies to assist HUAWEI's goal of reverse engineering Company 6's nonpublic technology: "The internal information of [Company 6's] controller chip is not open to us, and the public information from [Company 6] is relatively limited; We lack effective engineering methods for reverse

analysis.” The document called for the creation of “reverse analysis engineering teams and laboratories” and reliance on “external resources,” such as the Professor, who could provide “third-party analysis materials,” as well as “external information.”

51. In or about December 2016, HUAWEI and the Professor entered into a contract calling for the Professor to develop prototype software for memory hardware. That same month, the Professor contacted Company 6 seeking access to a prototype board containing Company 6’s proprietary chip (the “Board”) for research purposes. At no time did the Professor disclose to Company 6 the existence of his contract or his relationship with HUAWEI.

52. In or about February 2017, Company 6 agreed to license a Board to the Professor. Company 6 would not have agreed to provide a Board to the Professor had the Professor disclosed the existence of his relationship with HUAWEI, because HUAWEI was a direct competitor of Company 6 in the field of memory architecture.

53. In the licensing agreement executed in or about February 2017 (the “Agreement”), the Professor and Company 6 agreed that the Professor’s access to a Board was conditioned on, among other requirements, the following prohibitions: (1) the direct or indirect transfer of rights or usage in the Board to third parties; (2) the modification or creation of derivative works based on the Board; and (3) the disclosure, divulgence or publication of the Board and its underlying technology. Pursuant to the Agreement, Company 6 provided the Professor with a specific product number and the identity of its PRC-based distributor of the Board (the “Distributor”), both of which were considered sensitive proprietary information.

54. Supply chain issues ultimately prevented Company 6 from delivering a Board to the Professor immediately after execution of the Agreement. In or about April 2017, approximately two months after execution of the Agreement, the Professor contacted Company 6 and claimed that he/she needed the Board immediately because of the availability of students to assist with research. In actuality, the Professor sought immediate delivery of the Board because of a pending project that the Professor had with HUAWEI. Indeed, that same month, the Professor wrote HUAWEI that “[t]he current dilemma is that the equipment [from Company 6] is not yet available”—thus making the Professor’s research impossible.

55. In or about April 2017, after obtaining a Board from Company 6, the Professor provided HUAWEI with the product number for the Board, as well as the identity of the Distributor, in violation of the Agreement. HUAWEI used this information to try on at least two occasions to acquire a Board from the Distributor without first contacting Company 6, but the Distributor refused to sell a Board to HUAWEI without Company 6’s consent. After the Distributor informed Company 6 about these efforts by HUAWEI, Company 6 contacted the Professor, who falsely denied providing the product number and the identity of the Distributor to HUAWEI. Company 6 also contacted HUAWEI, which refused to answer Company 6’s query as to how HUAWEI obtained information regarding the product number and the identity of the Distributor.

56. Also in violation of the terms of the Agreement, the Professor provided HUAWEI with performance results of the Professor’s testing of the Board. This information would have assisted in HUAWEI’s efforts to reverse engineer Company 6’s proprietary technology.

57. In or about July 2017, HUAWEI requested a high-level meeting with Company 6 to discuss Company 6's proprietary technology, ostensibly to develop a commercial relationship with Company 6. However, an internal HUAWEI email indicated that HUAWEI's actual motivation for the meeting was to "[o]btain the [Board] and support the development of our two projects" with the Professor. During the meeting, HUAWEI requested several samples of the Board, but Company 6 responded that it would not release a Board to HUAWEI without a nondisclosure agreement. At no time during these negotiations did HUAWEI disclose its relationship with the Professor or that it was seeking samples of the Board in connection with the Professor's work or its collaboration with the Professor. HUAWEI never established a commercial partnership with Company 6.

58. The efforts to misappropriate the intellectual property of Company 6 were designed to permit HUAWEI to save on research and development costs in the development of its own architecture for memory hardware.

III. False Statements to the U.S. Government

59. As part of the efforts by the defendant HUAWEI to establish and operate its business, particularly in the United States, the IP Defendants and their agents and representatives made repeated false statements to the U.S. government about their efforts to misappropriate the intellectual property of the Victim Companies, as well as the nature and the scope of HUAWEI's business activities related to sanctioned countries such as Iran and North Korea, to avoid the economic and regulatory consequences of making truthful statements, including the restriction of HUAWEI from U.S. markets and business opportunities.

60. In or about July 2007, agents with the Federal Bureau of Investigation (“FBI”) interviewed Individual-1 in New York, New York.

a. During the interview, among other things, Individual-1 falsely stated, in substance and in part, that HUAWEI did not conduct any activity in violation of U.S. export laws and that HUAWEI operated in compliance with all U.S. export laws. Individual-1 also falsely stated, in substance and in part, that HUAWEI had not dealt directly with any Iranian company. Individual-1 further stated that he believed HUAWEI had sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran.

b. During the same interview, Individual-1 falsely stated, in substance and in part, that HUAWEI “won” the lawsuit with Company 1 and that the FBI should consult with the Chief Executive Officer (“CEO”) of Company 1, who would “testify” that HUAWEI did not engage in intellectual property rights violations.

61. In or about 2012, the U.S. House of Representatives’ Permanent Select Committee on Intelligence (the “HPSCI”) conducted an investigation (the “HPSCI Investigation”) and hearings related to “National Security Threats from Chinese Telecommunications Companies Operating in the United States.” The purpose of the investigation was to consider, in relevant part, potential threats posed by HUAWEI as it sought to expand its business in the United States.

62. On or about September 13, 2012, a “corporate senior vice president under the chief Huawei representative to the United States” who also claimed to have the title of “President of Huawei North America” (the “Senior Vice President”), an individual whose identity is known to the Grand Jury, testified before the HPSCI. At the start of his testimony, the Senior Vice President identified the economic importance of the hearing for

HUAWEI, explaining that HUAWEI's "U.S. business has been damaged by unsubstantiated, non-specific concerns suggesting that Huawei poses a security threat."

a. During his testimony, in response to questions about HUAWEI's theft of trade secrets from Company 1, the Senior Vice President falsely testified that "Huawei provided our source code [for] our product to [Company 1] for review. And the result is there was not any infringement found." The Senior Vice President further falsely testified that the "source code" was "actually from a third party partner . . . already available and opened on the Internet."

b. Also during his testimony, the Senior Vice President falsely testified that HUAWEI's business in Iran had not "violated any laws and regulations including sanction-related requirements," and that "We have never provided any equipment to the Iranian government. All that we have provided are only for commercial civilian use." In fact, HUAWEI's business in Iran did violate laws and regulations, including sanction-related requirements, and included the provision of goods and services to the Iranian government, including surveillance technology used to monitor, identify and detain protestors during anti-government demonstrations in Tehran, Iran in or about 2009.

63. To supplement the testimony of the Senior Vice President, HUAWEI submitted, among other documents, a chart falsely reflecting "No Huawei Entities or Affiliates involved in Business activities" in North Korea and approximately \$19 million in "sales by distributors and resellers" to North Korea in 2008 and 2009. The chart did not reflect any activity in North Korea after 2009. In fact, HUAWEI was involved in business activities in North Korea, including numerous telecommunications projects, beginning no later than 2008. The chart also listed several HUAWEI clients in Iran, but omitted other

large HUAWEI clients with connections to the Government of Iran being served by SKYCOM.

IV. The Scheme to Defraud Financial Institutions

A. The Victim Financial Institutions

64. Financial Institution 1, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Its United States-based subsidiary (“U.S. Subsidiary 1”), an entity the identity of which is known to the Grand Jury, was a federally chartered bank, the deposits of which were insured by the Federal Deposit Insurance Company (“FDIC”). Among the services offered by Financial Institution 1 to its clients were U.S.-dollar clearing through U.S. Subsidiary 1 and other financial institutions located in the United States, and Euro clearing through Financial Institution 1 subsidiaries and other financial institutions located in Eurozone countries. Between approximately 2010 and 2014, Financial Institution 1 and U.S. Subsidiary 1 cleared more than \$100 million worth of transactions related to SKYCOM through the United States. In or about 2017, Financial Institution 1 verbally communicated to HUAWEI representatives that it was terminating its banking relationship with HUAWEI.

65. Financial Institution 2, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 2 to its clients were U.S.-dollar clearing through a Financial Institution 2 subsidiary and other financial institutions located in the

United States, and Euro clearing through Financial Institution 2 subsidiaries and other financial institutions located in Eurozone countries.

66. Financial Institution 3, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 3 to its clients were U.S.-dollar clearing through Financial Institution 3 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 3 subsidiaries and other financial institutions located in Eurozone countries.

67. Financial Institution 4, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 4 to its clients were U.S.-dollar clearing through Financial Institution 4 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 4 subsidiaries and other financial institutions located in Eurozone countries. A subsidiary of Financial Institution 4 (“U.S. Subsidiary 4”), an entity the identity of which is known to the Grand Jury, was a financial institution organized in the United States offering banking and financial services throughout the world. U.S. Subsidiary 4 offered HUAWEI and its affiliates banking services and cash management services, including for accounts in the United States.

B. HUAWEI's Business in Countries Subject to Sanctions

68. As part of its international business model, HUAWEI participated in business in countries subject to U.S., E.U. and/or U.N. sanctions, such as Iran. This business, which included arranging for shipment of HUAWEI goods and services to end users in sanctioned countries, was typically conducted through local affiliates in the sanctioned countries, such as SKYCOM in Iran.

69. Reflecting the inherent sensitivity of conducting business in jurisdictions subject to U.S., E.U. and/or U.N. sanctions, internal HUAWEI documents referred to such jurisdictions with code names. For example, the code "A2" referred to Iran, and "A9" referred to North Korea. HUAWEI internal documents sometimes referred to those countries solely by code name, rather than by country name. HUAWEI internal documents did not refer to countries that were not subject to sanctions, such as the United States or Canada, by similar code names.

C. The SKYCOM Fraudulent Scheme

70. Even though the U.S. Department of the Treasury's Office of Foreign Assets Control's ("OFAC") Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. Part 560, proscribed the export of U.S.-origin goods, technology and services to Iran and the Government of Iran, HUAWEI operated SKYCOM as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for HUAWEI's Iran-based business while concealing the link to HUAWEI. HUAWEI could thus attempt to claim ignorance with respect to any illegal act committed by SKYCOM on behalf of HUAWEI, including violations of the ITSR and other applicable U.S. law. In addition, HUAWEI assisted the Government of Iran by installing surveillance

equipment, including surveillance equipment used to monitor, identify and detain protestors during the anti-government demonstrations of 2009 in Tehran, Iran. Moreover, contrary to U.S. law, SKYCOM, on behalf of HUAWEI, employed in Iran at least one U.S. citizen (“Employee-1”), an individual whose identity is known to the Grand Jury.

71. Since in or about July 2007, HUAWEI repeatedly misrepresented to the U.S. government and to various victim financial institutions, including Financial Institutions 1, 2, 3 and 4, and their U.S. and Eurozone subsidiaries and branches (collectively, the “Victim Institutions”), that, although HUAWEI conducted business in Iran, it did so in a manner that did not violate applicable U.S. law, including the ITSR. In reality, HUAWEI conducted its business in Iran in a manner that violated applicable U.S. law, which includes the ITSR. Had the Victim Institutions known about HUAWEI’s repeated violations of the ITSR, they would have reevaluated their banking relationships with HUAWEI, including their provision of U.S.-dollar and Euro clearing services to HUAWEI.

72. Additionally, HUAWEI repeatedly misrepresented to Financial Institution 1 that HUAWEI would not use Financial Institution 1 and its affiliates to process any transactions regarding HUAWEI’s Iran-based business. In reality, HUAWEI used U.S. Subsidiary 1 and other financial institutions operating in the United States to process U.S.-dollar clearing transactions involving millions of dollars in furtherance of HUAWEI’s Iran-based business. Some of these transactions passed through the Eastern District of New York.

73. In or about 2011 and early 2012, news reports in The Wall Street Journal and Reuters claimed that HUAWEI assisted the Government of Iran to perform domestic surveillance, including providing equipment to track persons’ locations and a

surveillance system to monitor landline, mobile and internet communications. In response to the claims in The Wall Street Journal, HUAWEI issued an official press release in or about December 2011 through its website titled “Statement Regarding Inaccurate and Misleading Claims about Huawei’s Commercial Operations in Iran.” In the press release, HUAWEI claimed it “is not capable of ‘overseeing’ the network as reported in the article and we have no involvement in any type of monitoring and filtering activities.”

74. Similarly, in or about late 2012 and early 2013, various news organizations, including Reuters, reported that SKYCOM had sold and attempted to sell embargoed U.S.-origin goods to Iran in violation of U.S. law, and that HUAWEI in fact owned and operated SKYCOM. In December 2012, Reuters published an article purporting to contain a HUAWEI official statement addressing and denying those allegations. In January 2013, Reuters published a second article purporting to contain a HUAWEI official statement, again addressing and denying the Iran allegations. The purported statements by HUAWEI in these articles were relied on by the Victim Institutions in determining whether to continue their banking relationships with HUAWEI and its subsidiaries

75. Following publication of the December 2012 and January 2013 Reuters articles, various HUAWEI representatives and employees communicated to the Victim Institutions and to the public that the allegations regarding HUAWEI’s ownership and control of SKYCOM were false and that, in fact, HUAWEI did comply with applicable U.S. law, which includes the ITSR. Based in part on these false representations, the Victim Institutions continued their banking relationships with HUAWEI and its subsidiaries and affiliates.

76. For example, in or about June 2013, the defendant WANZHOU MENG requested an in-person meeting with a Financial Institution 1 executive (the “Financial Institution 1 Executive”), an individual whose identity is known to the Grand Jury. During the meeting, which took place on or about August 22, 2013, MENG spoke in Chinese, relying in part on a PowerPoint presentation written in Chinese. Upon request by the Financial Institution 1 Executive, MENG arranged for an English-language version of the PowerPoint presentation to be delivered to Financial Institution 1 on or about September 3, 2013.

77. In relevant part, the PowerPoint presentation included numerous misrepresentations regarding HUAWEI’s ownership and control of SKYCOM and HUAWEI’s compliance with applicable U.S. law, including that (1) HUAWEI “operates in Iran in strict compliance with applicable laws, regulations and sanctions of UN, US and EU”; (2) “Huawei has never provided and will never provide any technology, product, or service for monitoring communications flow, tracking user locations, or filtering media contents in the Iranian market”; (3) “HUAWEI’s engagement with SKYCOM is normal business cooperation”; (4) the defendant WANZHOU MENG’s participation on the Board of Directors of SKYCOM was to “help HUAWEI to better understand SKYCOM’s financial results and business performance, and to strengthen and monitor SKYCOM’s compliance”; and (5) “HUAWEI subsidiaries in sensitive countries will not open accounts at [Financial Institution 1], nor have business transactions with [Financial Institution 1].” These statements were all false.

78. In early 2014, several months after the meeting with Financial Institution 1 Executive, the defendant WANZHOU MENG traveled to the United States,

arriving at John F. Kennedy International Airport, which is located in the Eastern District of New York. When she entered the United States, MENG was carrying an electronic device that contained a file in unallocated space—indicating that the file may have been deleted—containing the following text:

Suggested Talking Points

The core of the suggested talking points regarding Iran/Skycom: Huawei's operation in Iran comports with the laws, regulations and sanctions as required by the United Nations, the United States and the European Union. The relationship with Skycom is that of normal business cooperation. Through regulated trade organizations and procedures, Huawei requires that Skycom promises to abide by relevant laws and regulations and export controls. Key information 1: In the past — ceased to hold Skycom shares 1, With regards to cooperation: Skycom was established in 1998 and is one of the agents for Huawei products and services. Skycom is mainly an agent for Huawei.

Other text in the same file appeared to refer to a document announcing the appointment of Huawei employees that was “signed by MENG Wanzhou,” the defendant.

79. Based in part on the false representations made by the defendant WANZHOU MENG and others, Financial Institution 1 continued its banking relationship with HUAWEI and its subsidiaries and affiliates.

D. The North Korea Fraudulent Scheme

80. Some of the Victim Institutions asked HUAWEI about HUAWEI's business presence in North Korea to better understand the risk, both reputational and legal, in processing HUAWEI transactions.

81. HUAWEI representatives and employees repeatedly denied to some of the Victim Institutions that HUAWEI was involved in numerous projects in North Korea. For example, in or about March 2013, HUAWEI employees told representatives of Financial

Institution 4 that, in sum and substance, HUAWEI had no business in North Korea. These representations were false.

82. In fact, HUAWEI was involved in numerous projects in North Korea beginning no later than 2008. Indeed, internal HUAWEI documents referred to the geographic location of projects in North Korea with the code “A9”—HUAWEI’s code for North Korea. HUAWEI employees took steps to conceal HUAWEI’s involvement in projects in North Korea. For example, shipping instructions provided by HUAWEI to a supplier in 2013 included the instruction that, for shipments to “A9/NK/NORTH KOREA,” there should be “No HW [HUAWEI] logo,” indicating that HUAWEI’s corporate logo should not be included on shipments destined for North Korea.

E. HUAWEI’s Continued Scheme to Defraud Financial Institutions

83. In or about 2017, Financial Institution 1 decided to terminate its global relationship with HUAWEI because of risk concerns regarding HUAWEI’s business practices. During a series of meetings and communications, Financial Institution 1 repeatedly communicated to HUAWEI that the decision to terminate its banking relationship with HUAWEI had been made by Financial Institution 1 alone, and was not a mutual decision with HUAWEI.

84. After learning of Financial Institution 1’s decision to terminate its relationship with HUAWEI, HUAWEI took steps to secure and expand its banking relationships with other financial institutions, including U.S. Subsidiary 4. In doing so, HUAWEI employees made material misrepresentations to U.S. Subsidiary 4, among other financial institutions, regarding the reason for the termination of its relationship with Financial Institution 1 and the party responsible for the termination, claiming that HUAWEI,

not Financial Institution 1, had initiated the termination. Specifically, in meetings and correspondence with representatives of U.S. Subsidiary 4, HUAWEI employees, [REDACTED]

[REDACTED] falsely represented that HUAWEI was considering terminating its relationship with Financial Institution 1 because HUAWEI was dissatisfied with Financial Institution 1's level of service. HUAWEI's misrepresentation that it had decided to terminate its relationship with Financial Institution 1 was communicated to various components of U.S. Subsidiary 4, including in the Eastern District of New York.

85. Based in part on these false representations and omissions made by the defendants HUAWEI, [REDACTED], among other HUAWEI employees, U.S. Subsidiary 4 undertook to expand its banking relationship with HUAWEI and its subsidiaries and affiliates, and continued to maintain its existing banking relationship with HUAWEI globally, including in the United States. Had the defendants told U.S. Subsidiary 4 the truth about Financial Institution 1's decision to terminate its relationship with HUAWEI, U.S. Subsidiary 4 would have reevaluated its relationship with HUAWEI and its subsidiaries and affiliates.

86. By avoiding the termination of HUAWEI's relationship with Financial Institution 4 and U.S. Subsidiary 4, HUAWEI received income indirectly in the form of cost savings and the value of continued banking services, the proceeds of which income were used to operate and grow HUAWEI's business.

F. The Scheme to Obstruct Justice

87. In or about 2017, HUAWEI and HUAWEI DEVICE USA became aware of the U.S. government's criminal investigation of HUAWEI and its affiliates. In

response to the investigation, HUAWEI and HUAWEI DEVICE USA made efforts to move witnesses with knowledge about HUAWEI's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and to destroy and conceal evidence in the United States of HUAWEI's Iran-based business. By impeding the government's investigation, HUAWEI and HUAWEI DEVICE USA sought to avoid criminal prosecution with respect to HUAWEI's Iran-based activities, which would subject HUAWEI and its U.S. affiliates and subsidiaries, including HUAWEI DEVICE USA, to the threat of economic harm.

COUNT ONE
(Racketeering Conspiracy)

88. The allegations contained in paragraphs one through 87 are realleged and incorporated as if fully set forth in this paragraph.

89. At all times relevant to this Superseding Indictment, HUAWEI and its parents, global affiliates and subsidiaries, including HUAWEI DEVICE, HUAWEI DEVICE USA, FUTUREWEI and SKYCOM, constituted an "enterprise," as defined in Title 18, United States Code, Section 1961(4), that is, a group of legal entities associated in fact (hereinafter, the "Huawei Enterprise"). The Huawei Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

90. The principal purpose of the Huawei Enterprise was to grow the global "Huawei" brand into one of the most powerful telecommunications equipment and consumer electronics companies in the world by entering, developing and dominating the markets for telecommunications and consumer electronics technology and services in each of the countries in which the Huawei Enterprise operated.

91. The Huawei Enterprise operated in the Eastern District of New York, the Central District of California, the District of Columbia, the District of Delaware, the District of New Jersey, the Eastern District of Texas, the Northern District of California, the Northern District of Illinois, the Northern District of Texas, the Southern District of California, the Southern District of New York, the Western District of New York, the Western District of Washington and elsewhere, including overseas.

92. In or about and between 1999 to the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE USA and FUTUREWEI, together with others, did knowingly and intentionally conspire to violate Title 18, United States Code, Section 1962(a), that is, to use and invest, directly and indirectly, a part of income and the proceeds of income, to wit: income received by HUAWEI, HUAWEI DEVICE USA and FUTUREWEI and derived, directly and indirectly, from a pattern of racketeering activity, in which HUAWEI, HUAWEI DEVICE USA and FUTUREWEI participated as principals within the meaning of Title 18, United States Code, Section 2, in the establishment and operation of the Huawei Enterprise, an enterprise that engaged in, and the activities of which affected, interstate and foreign commerce.

93. The pattern of racketeering activity, as defined in Title 18, United States Code, Sections 1961(1) and 1961(5), consisted of multiple acts indictable under Title 18, United States Code, Sections 1343 (relating to wire fraud), 1344 (relating to financial institution fraud), 1503 (relating to obstruction of justice), 1512 (relating to tampering with a witness, victim or an informant), 1832 (relating to theft of trade secrets), 1956 (relating to the

laundering of monetary instruments), and 2319 (relating to criminal infringement of a copyright). The manner and means of the above-described conspiracy include the allegations set forth in paragraphs one through 87, which are realleged and incorporated as if fully set forth in this paragraph.

(Title 18, United States Code, Sections 1962(d) and 3551 et seq.)

COUNT TWO
(Conspiracy to Steal Trade Secrets)

94. The allegations contained in paragraphs one through three and eight through 63 are realleged and incorporated as if fully set forth in this paragraph.

95. In or about and between 2000 and the present, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, knowingly, and with intent to convert one or more trade secrets that were related to a product used in or intended for use in interstate and foreign commerce, conspired to (a) steal, and without authorization appropriate, take, carry away and conceal, and obtain by fraud, artifice and deception such trade secrets, (b) without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate and convey such trade secrets, (c) receive, buy and possess such trade secrets, knowing the same to have been stolen and appropriated, obtained and converted without authorization, to the economic benefit of HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, and intending or knowing that the offense would injure any owner of those trade secrets, to wit: the trade secrets of the

Victim Companies, all contrary to Title 18, United States Code, Sections 1832(a)(1), 1832(a)(2) and 1832(a)(3).

96. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, committed and caused the commission of, among others, the following:

OVERT ACTS

a. In or about March 2002, an employee of FUTUREWEI, an individual whose identity is known to the Grand Jury, contacted an employee of Company 1, an individual whose identity is known to the Grand Jury, regarding potential employment with FUTUREWEI, in an attempt to misappropriate trade secret information of Company 1.

b. On or about March 3, 2003, at the request of HUAWEI, Engineer-1, an employee of Company 2, wrote an email to Individual-1 and Individual-2, both employed by HUAWEI, and attached a Company 2 document, which comprised and included trade secret information, bearing the markings “HIGHLY CONFIDENTIAL” and “[Company 2] Confidential Property.”

c. On or about July 11, 2007, Individual-1 stated to FBI agents that HUAWEI had “won” the lawsuit with Company 1 and that the CEO of Company 1 would “testify” that HUAWEI did not engage in intellectual property rights violations.

d. On or about October 30, 2009, FUTUREWEI filed a provisional patent application with the U.S. Patent and Trademark Office that used and relied upon in large part misappropriated Company 4 trade secret information.

e. On or about September 13, 2012, the Senior Vice President falsely testified before U.S. Congress that “As specifically to the source code [allegedly stolen from Company 1], the source code of the issues was actually from a third party partner . . . already available and open on the internet.”

f. On or about May 29, 2013, a HUAWEI DEVICE USA employee accessed a Company 5 laboratory and surreptitiously placed a robot arm, which comprised and included trade secret information of Company 5, into a laptop bag and secreted the robot arm from the laboratory.

g. In or about July 2013, HUAWEI and HUAWEI DEVICE launched a formal policy to encourage employees to steal confidential information from competitors.

h. On or about June 9, 2015, Company 6 emailed a presentation marked “Proprietary and Confidential” to HUAWEI describing Company 6’s architecture for solid state drives, which HUAWEI personnel distributed internally, notwithstanding oral promises to maintain confidentiality and not to distribute the information to HUAWEI engineers.

i. On or about June 18 and 21, 2017, HUAWEI tried unsuccessfully to purchase Company 6’s nonpublic proprietary technology directly from the Distributor without Company 6’s permission and without informing Company 6.

j. On or about August 2, 2017, the Professor emailed testing results of software run on the Board to HUAWEI, contrary to the Agreement between the Professor and Company 6, which expressly prohibited the direct or indirect transfer of rights or usage in the Board to third parties.

k. In or about 2017, HUAWEI circulated an internal memorandum calling for the use of reverse engineering teams which would rely on external resources to obtain third-party analysis of nonpublic intellectual property belonging to other companies.

(Title 18, United States Code, Sections 1832(a)(5), 1832(b) and 3551 et seq.)

COUNT THREE

(Conspiracy to Commit Wire Fraud)

97. The allegations contained in paragraphs one through three and eight through 63 are realleged and incorporated as if fully set forth in this paragraph.

98. In or about and between 2009 and the present, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the Victim Companies, and to obtain money and property from the Victim Companies, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FOUR

(Conspiracy to Commit Bank Fraud)

99. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

100. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FIVE
(Conspiracy to Commit Bank Fraud)

101. The allegations contained in paragraphs one, six, seven, 64 through 79, and 83 through 86 are realleged and incorporated as if fully set forth in this paragraph.

102. In or about and between August 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, [REDACTED]
[REDACTED] together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent

pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT SIX

(Conspiracy to Commit Wire Fraud)

103. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

104. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT SEVEN

(Bank Fraud)

105. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

106. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the

defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT EIGHT
(Bank Fraud)

107. The allegations contained in paragraphs one, six, seven, 64 through 79, and 83 through 86 are realleged and incorporated as if fully set forth in this paragraph.

108. In or about and between August 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, [REDACTED] [REDACTED] together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT NINE
(Wire Fraud)

109. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

110. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: the defendants HUAWEI, SKYCOM and MENG, together with others, (a) made, and caused to be made, a series of misrepresentations through email communications, written communications otherwise conveyed through the wires, and oral communications made with knowledge that the oral communications would be memorialized and subsequently transmitted through the wires, about, among other things, the relationship between HUAWEI and SKYCOM, HUAWEI’s compliance with U.S. and U.N. laws and regulations, and the kinds of financial transactions in which HUAWEI engaged through the Victim Institutions; and (b) as a result of the misrepresentations, caused a series of wires to be sent by financial institutions from outside of the United States through the United States.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT TEN
(Conspiracy to Defraud the United States)

111. The allegations contained in paragraphs one, four, and 64 through 87 are realleged and incorporated as if fully set forth in this paragraph.

112. In or about and between July 2007 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful governmental functions and operations of OFAC, an agency of the United States, in the enforcement of economic sanctions laws and regulations administered by that agency and the issuance by that agency of appropriate licenses relating to the provision of financial services.

113. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, committed and caused the commission of, among others, the following:

OVERT ACTS

a. On or about July 11, 2007, Individual-1 stated to FBI agents that HUAWEI did not conduct any activity in violation of U.S. export laws, that HUAWEI operated in compliance with all U.S. export laws, that HUAWEI had not dealt directly with any Iranian company and that he believed HUAWEI had sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran.

b. On or about September 13, 2012, the Senior Vice President testified before U.S. Congress that HUAWEI's business in Iran had not "violated any laws and regulations including sanction-related requirements."

c. On or about September 17, 2012, the Treasurer of HUAWEI met with a principal of U.S. Subsidiary 4, an individual whose identity is known to the Grand

Jury, in New York, New York, and informed U.S. Subsidiary 4 that HUAWEI and its global affiliates did not violate any applicable U.S. law.

d. On or about July 24, 2013, SKYCOM caused U.S. Subsidiary 1 to process a U.S.-dollar clearing transaction of \$52,791.08.

e. On or about July 24, 2013, SKYCOM caused a bank located in the Eastern District of New York ("Bank 1"), an entity the identity of which is known to the Grand Jury, to process a U.S.-dollar clearing transaction of \$94,829.82.

f. On or about August 20, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of \$14,835.22.

g. On or about August 28, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of \$32,663.10.

h. On or about April 11, 2014, SKYCOM caused a bank located in the United States ("Bank 2"), an entity the identity of which is known to the Grand Jury, to process a U.S.-dollar clearing transaction of \$118,842.45.

i. In or about April 2018, HUAWEI made efforts to move an employee ("Individual-4"), an individual whose identity is known to the Grand Jury, with knowledge about HUAWEI's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT ELEVEN
(Conspiracy to Violate IEEPA)

114. The allegations contained in paragraphs one, four, 64 through 67, 70 through 79 are realleged and incorporated as if fully set forth in this paragraph.

115. Through the International Emergency Economic Powers Act (“IEEPA”), the President of the United States was granted authority to address unusual and extraordinary threats to the national security, foreign policy or economy of the United States. 50 U.S.C. § 1701(a). Under IEEPA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any license, order, regulation or prohibition issued pursuant to the statute. 50 U.S.C. §§ 1705(a) and 1705(c).

116. To respond to the declaration by the President of a national emergency with respect to Iran pursuant to IEEPA, which was most recently continued in March 2018 (83 Fed. Reg. 11,393 (Mar. 14, 2018)), OFAC issued the ITSR. Absent permission from OFAC in the form of a license, these regulations prohibited, among other things:

a. The exportation, reexportation, sale or supply from the United States, or by a U.S. person, wherever located, of any goods, technology or services to Iran and the Government of Iran (31 C.F.R. § 560.204);

b. Any transaction by a U.S. person, wherever located, involving goods, technology or services for exportation, reexportation, sale or supply, directly or indirectly, to Iran or the Government of Iran (31 C.F.R. § 560.206); and

c. Any transaction by a U.S. person, or within the United States, that evaded or avoided, had the purpose of evading or avoiding, attempted to violate, or caused a violation of any of the prohibitions in the ITSR (31 C.F.R. § 560.203).

117. The ITSR prohibited providing financial services, including U.S. dollar-clearing services, to Iran or the Government of Iran. 31 C.F.R. §§ 560.204, 560.427. In addition, the prohibition against the exportation, reexportation, sale or supply of services applied to services performed on behalf of a person in Iran or the Government of Iran, or

where the benefit of such services was otherwise received in Iran, if the services were performed (a) in the United States by any person; or (b) outside the United States by a United States person, including an overseas branch of an entity located in the United States. 31 C.F.R. § 560.410.

118. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT TWELVE
(IEEPA Violations)

119. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

120. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods,

technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT THIRTEEN
(Conspiracy to Violate IEEPA)

121. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

122. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee-1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT FOURTEEN
(IEEPA Violation)

123. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

124. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee-1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT FIFTEEN
(Money Laundering Conspiracy)

125. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

126. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and intentionally conspire to transport, transmit and transfer monetary instruments and funds, to wit: wire transfers, from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit: conspiracy to violate IEEPA, in violation of Title

50, United States Code, Section 1705, all contrary to Title 18, United States Code, Section 1956(a)(2)(A).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT SIXTEEN
(Conspiracy to Obstruct Justice)

127. The allegations contained in paragraphs one, three, 64 through 82, and 87 are realleged and incorporated as if fully set forth in this paragraph.

128. In or about and between January 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and HUAWEI DEVICE USA, together with others, did knowingly, intentionally and corruptly conspire to obstruct, influence and impede an official proceeding, to wit: a Federal Grand Jury investigation in the Eastern District of New York, contrary to Title 18, United States Code, Section 1512(c)(2).

(Title 18, United States Code, Sections 1512(k) and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION AS TO COUNT ONE

129. The United States hereby gives notice to the defendants charged in Count One that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 1963(a), which requires any person convicted of such offense to forfeit: (a) any interest the person acquired or maintained in violation of Title 18, United States Code, Section 1962; (b) any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over any enterprise which the person has established, operated, controlled, conducted or participated in the conduct of, in violation of Title 18, United States Code, Section 1962; and (c) any

property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from racketeering activity in violation of Title 18, United States Code, Section 1962.

130. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 1963(m), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 1963(a) and 1963(m))

CRIMINAL FORFEITURE ALLEGATION AS TO COUNT TWO

131. The United States hereby gives notice to the defendants charged in Count Two that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 2323(b)(1), of (a) any article, the making or trafficking of which is prohibited under Title 17, United States Code, Section 506; Title 18, United States Code, Section 2318, 2319, 2319A, 2319B or 2320; or Chapter 90 of Title 18 of the United States Code; (b) any property used, or intended to be used, in any manner or part to commit or facilitate the commission of such offense; or (c) any property

constituting, or derived from, any proceeds obtained directly or indirectly as a result of such offense.

132. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 2323(b)(2), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 2323(b)(1) and 2323(b)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS THREE THROUGH NINE

133. The United States hereby gives notice to the defendants charged in Counts Three through Nine that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(2), which requires any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

134. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2) and 982(b)(1); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS TEN THROUGH FOURTEEN AND SIXTEEN

135. The United States hereby gives notice to the defendants charged in Counts Ten through Fourteen and Sixteen and that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

136. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT FIFTEEN

137. The United States hereby gives notice to the defendants charged in Count Fifteen that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property.

138. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;

- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek

forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21,
United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

DEBORAH L. CONNOR
CHIEF
MONEY LAUNDERING AND ASSET RECOVERY SECTION
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

CHIEF
COUNTERINTELLIGENCE AND EXPORT CONTROL SECTION
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE

F. # 2017R05903
FORM DBD-34
JUN. 85

No.
UNITED STATES DISTRICT COURT
EASTERN *District of* NEW YORK
CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA INC., FUTUREWEI TECHNOLOGIES, INC.,
SKYCOM TECH CO. LTD., WANZHOU MENG, also known as "Cathy
Meng" and "Sabrina Meng," [REDACTED]

Defendants.

SUPERSEDING INDICTMENT

(T. 18, U.S.C., §§ 371, 981(a)(1)(C); 982(a)(1), 982(a)(2), 982(b)(1),
1343, 1344, 1349, 1512(k), 1956(h), 1962(d), 1963(a), 1963(m),
2323(b)(1), 2323(b)(2), 2 and 3551 *et seq.*; T. 21, U.S.C., § 853(p); T. 28,
U.S.C., § 2461(c); T. 50, U.S.C., §§ 1702, 1705(a) and 1705(c))

A true bill.

[REDACTED]
Foreperson

Filed in open court this _____ day of _____ A.D. 20 ____

Clerk

Bail, \$ _____

*Alexander A. Solomon, Julia Nestor, David K. Kessler, and Sarah
Evans, Assistant U.S. Attorneys (718) 254-7000*

EXHIBIT M

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon.
 :
 v. : Crim. No.: 19-
 :
 DANDONG HONGXIANG : 18 U.S.C. §§ 371, 1956(h), and 2
 INDUSTRIAL DEVELOPMENT : 50 U.S.C. § 1705(c)
 CO. LTD., :
 MA XIAOHONG, :
 ZHOU JIANSHU, :
 LUO CHUANXU, and :
 HONG JINHUA :

INDICTMENT

Count One

**(Conspiracy to Violate the International Emergency Economic Powers Act
and Defraud the United States)**

The Grand Jury in and for the District of New Jersey, sitting at Newark,
charges:

Introduction

At all times relevant to this Indictment:

1. The city of Dandong in the Liaoning province of the People's Republic of China was on the border with the Democratic People's Republic of Korea ("North Korea" or "DPRK"). It was one of the largest cities on the China-North Korea border and was a significant location for trade between China and North Korea.

2. The Korea Kwangsong Banking Corporation ("KKBC"), a North Korean bank, maintained an office in Dandong.

3. In or about August 2009, KKBC was publicly named a “Specially Designated National” by the United States Department of the Treasury under Executive Order 13382, issued pursuant to the International Emergency Economic Powers Act (“IEEPA”). Accordingly, KKBC was prohibited from using the United States’ financial institutions for any reason, and it was a crime for anyone or any business entity to willfully assist KKBC in evading the prohibition. 50 U.S.C. § 1705.

Ma Xiaohong

4. Since in or about 1996, defendant MA XIAOHONG (“MA”) was engaged in trade with and on behalf of North Korea from her base in Dandong. In or about 2002, defendant MA opened up her own company for the purpose of trade with North Korea.

5. Defendant MA used a company she formed, the Liaoning Hongxiang Industrial Group, to operate a series of businesses, most of which use “Dandong Hongxiang” as part of their names. Such companies included Dandong Hongxiang Industrial Development (“DHID”), Dandong Hongxiang International Freight Forwarders, Dandong Hongxiang Travel Agency, and Dandong Hongxiang Real Estate, among others.

6. Defendant MA was the principal shareholder and senior executive of defendant DHID. As set forth below, she was also the sole owner and shareholder of many companies that served as front companies. Those front companies were created by or acquired by DHID employees for the purposes of transacting business in U.S. dollars for or on behalf of KKBC and other North

Korean entities while evading the U.S. government's prohibitions against such financial transactions.

Dandong Hongxiang Industrial Development Co, Ltd ("DHID")

7. Defendant DHID was a Chinese company whose core business was trade with North Korea.

8. According to a DHID PowerPoint presentation, defendant DHID was an enterprise that conducted North Korean import and export business, had a ten-year history of conducting business with North Korea, and had a trading value of 250 million U.S. dollars in 2010, which accounted for more than 20% of total trading volume between China and North Korea at that time. Further, according to the presentation, DHID's customers were: (a) companies affiliated with the North Korean Government who controlled the purchase of bulk goods and equipment, (b) North Korean representatives permanently residing in China who were sent to China by DPRK companies to make their own purchase orders, (c) China Commerce Department bidding projects to aid North Korea, and (d) small companies or individuals who did not have a license to import/export on their own, or needed to use DHID to get a better purchase price.

9. The presentation identified the DPRK as defendant DHID's primary customer. According to the presentation, in the three years after 2009, DHID's export volume to North Korea increased 30% annually and was likely to increase by more than 10% in the future. Further, the presentation identified

one of defendant DHID's disadvantages as business risks associated with the North Korean situation.

10. Due to defendant MA's close relationship with North Korean officials, she allowed her personal bank account to be used for DHID payments on behalf of a North Korean official in Russia who requested that transactions be conducted in U.S. dollars.

11. Since on or about August 2009, defendant DHID's growth in business related, at least in part, to its work on behalf of KKBC. Soon after the August 2009 designation of KKBC, which designation blocked the bank's access to the U.S. financial system, defendant DHID began making payments in U.S. dollars on behalf of KKBC, and these payments grew significantly over time. Defendant DHID's U.S. correspondent banking transactions increased from approximately \$1.3 million for the approximate three years prior to KKBC's designation to approximately \$110 million from 2011 to 2014, after KKBC was designated.

12. As set forth in more detail below, even after August 2009 when KKBC was designated, and defendant DHID and its co-conspirators knew of this designation, defendant DHID, the individual defendants, and their co-conspirators continued to engage in transactions in U.S. dollars through the U.S. financial system on behalf of KKBC and other North Korean entities.

Zhou Jianshu

13. Defendant ZHOU JIANSHU ("ZHOU") was the general manager of defendant DHID and worked directly for defendant MA. Defendant ZHOU, at

times coordinating with other DHID employees, established numerous front companies. The front companies were used to transact U.S. dollar financial transactions that cleared through the United States on behalf of KKBC, in violation of IEEPA. Defendant ZHOU incorporated several of the front companies using his own personal identifying information. Defendant ZHOU was the sole owner and shareholder of several such companies.

14. Defendant ZHOU oversaw both the logistics and payments for at least three separate U.S. dollar transactions conducted on behalf of KKBC. Those three transactions violated IEEPA. He also coordinated payments to goods and commodities companies in U.S. dollars, using defendant DHID and its front companies to conceal North Korea's identity as the purchaser of the goods and commodities.

Luo Chuanxu

15. Defendant LUO CHUANXU ("LUO") was a financial manager at DHID and served as an assistant to defendants MA and ZHOU. Defendant LUO was involved in the creation of front companies for the purpose of conducting U.S. dollar transactions on behalf of North Korea-based entities. Defendant LUO was also involved in making payments to vendors who supplied commodities to the DPRK. Defendant LUO was the CEO of at least two of the front companies established on behalf of DHID. For certain transactions, defendant LUO attempted to conceal the fact that North Korea was the supplier of commodities being exported from North Korea.

16. Defendant LUO communicated in coded language with potential buyers of North Korean goods in order to conceal the fact that North Korea was the source of the products.

Hong Jinhua

17. Defendant HONG JINHUA ("HONG") was the deputy general manager of DHID and worked directly for MA. Defendant HONG, at times coordinating with other DHID employees, registered front companies, and managed U.S. dollar bank account information on behalf of DHID and its front companies. Defendant HONG established several of the front companies using her own personal identifying information. Defendant HONG was the director of these companies.

18. During the period after KKBC was designated by the United States Department of the Treasury, defendant HONG maintained regular email contact with at least two different KKBC representatives, and played a role in managing the banking activities between defendant DHID and KKBC. Defendant HONG received KKBC bank statements summarizing U.S. dollar financial transactions between KKBC and defendant DHID. The bank statements were printed on official KKBC letterhead. The transactions reflected on the bank statements involved U.S. dollars moving into and out of a DHID account held at a KKBC branch in North Korea to fund commodity purchases made by DHID on behalf of North Korean trading companies that were funded or guaranteed by KKBC.

The International Emergency Economic Powers Act

19. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1701-1705, granted the President of the United States authority to deal with unusual and extraordinary threats to the national security, foreign policy or economy of the United States. 50 U.S.C. § 1701(a). The President was authorized to declare a national emergency and to impose economic sanctions in response to those threats. Under IEEPA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any license, order, regulation or prohibition issued pursuant to the Statute. 50 U.S.C. §§ 1705(a) and 1705(c).

20. On November 14, 1994, the President issued Executive Order 12938, finding "that the proliferation of nuclear, biological, and chemical weapons ("weapons of mass destruction") and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and [declaring] a national emergency to deal with that threat."

21. On June 28, 2005, the President issued Executive Order 13382 ("Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters") to target proliferators of weapons of mass destruction ("WMD") and their support networks and deny designated proliferators access to the U.S. financial and commercial systems.

22. Executive Order 13382 authorized the United States Secretary of the Treasury, in consultation with the Secretary of State, "to take such actions,

including the promulgation of rules and regulations, as may be necessary to carry out the purposes” of the Executive Order. Pursuant to that authority, on April 13, 2009, the Secretary of the Treasury promulgated the “Weapons of Mass Destruction Proliferators Sanctions Regulations” (the “WMDPSR”), 31 C.F.R. § 544.101 *et seq.*

The Weapons of Mass Destruction Proliferators Sanctions Regulations

23. Among other things, Executive Order 13382 and the WMDPSR:

a. Authorized the United States Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) to sanction individuals and entities facilitating the proliferation of weapons of mass destruction by placing such individuals or entities on the Specially Designated Nationals list, 31 C.F.R. § 544.201(a). As part of its enforcement efforts, OFAC published a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Collectively, such individuals and companies were called “Specially Designated Nationals” or “SDNs.” SDNs’ assets were blocked and U.S. persons were prohibited from dealing with them without first obtaining a license or other written authorization from OFAC. For purposes of Executive Order 13382 and the WMDPSR, a “U.S. person” included any entity such as a financial institution organized under the laws of the United States or any jurisdiction within the United States, 31 C.F.R. § 544.312.

b. Prohibited transactions or dealings, except as authorized or licensed by OFAC, by any U.S. person or within the United States with individuals and entities who had been placed on the SDN list, included (a) “[T]he

making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person [on the SDN list]"; and (b) "[T]he receipt of any contribution or provision of funds, goods, or services from any person [on the SDN list]," 31 C.F.R. § 544.201(b);

c. Prohibited any transaction by a U.S. person or within the United States that evaded or avoided, had the purpose of evading or avoiding, or attempted to violate any of the prohibitions set forth in Executive Order 13382 and the WMDPSR, 31 C.F.R. § 544.205; and,

d. Prohibited any non-U.S. person such as a corporation from causing financial or other services to be provided by a U.S. person for the benefit of a person or entity on the SDN list within the United States, except as authorized or licensed by OFAC, 31 C.F.R. § 544.405.

e. On August 11, 2009, OFAC designated KKBC pursuant to Executive Order 13382 as a Specially Designated National in connection with the proliferation of weapons of mass destruction, thereby subjecting KKBC to the prohibitions contained in 31 C.F.R. Part 544, Subpart B.

24. At no time before or after this designation in August 2009 did KKBC apply for, receive, or possess a license or authorization from OFAC to engage in any transaction or dealing with a U.S. person or within the United States.

North Korea's Banking Practices

25. North Korea needed to both sell certain commodities and buy commodities and services in international markets. To obtain goods and services in the international marketplace, North Korea needed access to U.S. dollars,

because certain international vendors preferred or required that purchases be made in U.S. dollars. When businesses engaged in U.S. dollar transactions overseas other than by the delivery of cash, those funds generally had to be moved through, or “cleared” through, a bank in the United States. Accordingly, to engage in U.S. dollar transactions, North Korea and North Korean entities needed access to the U.S. financial system.

26. A correspondent bank was a financial institution that provided financial services on behalf of another financial institution. Correspondent bank facilitated wire transfers, conducted business transactions, accepted deposits and gathered documents on behalf of other financial institutions. Correspondent banks were able to support international wire transfers for their customers in currencies that the foreign customer banks normally did not hold on reserve, such as U.S. dollars. Correspondent banks in the U.S. facilitated wire transfers by allowing foreign banks located exclusively overseas to maintain accounts at the correspondent banks in the United States. The funds used in foreign U.S. dollar transactions cleared through such accounts.

27. As a result of its designation in August 2009, KKBC lost access to both the U.S. financial system and to U.S. correspondent banks. Consequently, KKBC lost the ability to conduct transactions in U.S. dollars. After August 2009, KKBC illegally disguised its U.S. dollar transactions using non-designated entities such as DHID and its front companies. By conspiring with the defendants, and by using the front companies created by DHID, KKBC engaged

in financial transactions that transited the U.S. financial system, in violation of United States sanctions regulations and IEEPA.

The Conspiracy

28. From on or about December 9, 2009, through in or about September 2015, in Essex County, in the District of New Jersey and elsewhere, the defendants,

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT CO. LTD.,
MA XIAOHONG,
ZHOU JIANSHU,
LUO CHUANXU, and
HONG JINHUA,

and others did knowingly and intentionally conspire and agree with each other and others:

a. to violate, evade, and avoid the restrictions imposed by the Office of Foreign Assets Control, U.S. Department of the Treasury, under the Weapons of Mass Destruction Proliferators Sanctions Regulations, Title 31, Code of Federal Regulations, Section 544.101, *et seq.*, by providing services on behalf of and for the benefit of a Specially Designated National, to wit, Korea Kwangson Banking Corp. ("KKBC"), without first having obtained a license or other written authorization from the Office of Foreign Assets Control, and

b. to defraud the United States government by interfering with and obstructing a lawful government function, that is, the enforcement of the Weapons of Mass Destruction Proliferators Sanctions Regulations, by deceit, craft, trickery, and dishonest means, contrary to Title 50, United States Code,

Section 1705(c), and Title 31, Code of Federal Regulations, Sections 544.201 and 544.205.

Objects of the Conspiracy

29. The objects of the conspiracy were:

- a. To transact business on behalf of SDNs using U.S. financial institutions despite the legal prohibition against such transactions, and to profit from engaging in such transactions;
- b. To conceal from and mislead U.S. financial institutions that a non-designated entity was sending U.S. dollars to non-sanctioned commodity or goods traders; and
- c. To willfully evade or violate, and to cause others to evade or to violate the regulations and prohibitions, and licensing requirements of IEEPA, Executive Order 13382, and the WMDPSR.

Manner and Means Of The Conspiracy

30. It was a part of the conspiracy that after the designation of KKBC by U.S. Treasury Officials in August 2009, defendants MA, ZHOU, LUO, HONG and DHID created or acquired at least 22 front companies that were incorporated in Hong Kong, the British Virgin Islands, England, Seychelles, Wales and Anguilla, among others. For most of these companies, the defendants, or those close to them, were listed as the CEOs, directors, and sole shareholders. Many of the front companies shared the same addresses in the British Virgin Islands or in Hong Kong.

31. It was further a part of the conspiracy that the co-conspirators opened bank accounts held in the names of the front companies at 12 banks in China that maintained correspondent accounts with the U.S.

32. It was further a part of the conspiracy that the U.S. dollar transactions were conducted in the name of a front company, creating the appearance that the U.S. correspondent bank, for example, a British Virgin Islands ("BVI") or Hong Kong-based trading company, was sending U.S. dollars to a non-sanctioned commodity or goods trader somewhere outside the United States.

33. It was further a part of the conspiracy that U.S. correspondent banks would process transactions that would not have been processed had the correspondent banks known that KKBC had funded or guaranteed defendant DHID's front company.

34. It was further a part of the conspiracy that the bank accounts held by the front companies' accounts were funded by defendant DHID with U.S. dollars from designated parties in North Korea and were used to pay for purchases destined for North Korea. In this way, defendant DHID and the front companies acted as the business entities through which designated North Korean entities, such as KKBC, accessed the U.S. financial system.

35. It was further a part of the conspiracy that, at times, the front companies processed transactions funded or guaranteed by KKBC that transited through U.S. financial institutions.

36. It was further a part of the conspiracy that, at times, the defendants—using the front companies they controlled—managed the full logistical chain of supply and payment for commodity contracts that were in fact guaranteed or funded by KKBC for North Korea-based entities. The defendants did so to ensure the performance and payment of specific commodity purchases that were made in U.S. dollars. In the course of the conspiracy, one or more of the correspondent processing centers involved in the international wire transfers on behalf of or for the benefit of KKBC described herein were located in the District of New Jersey.

37. It was further a part of the conspiracy that the prices the defendants charged for goods purchased by KKBC or with its guarantees were substantially higher than the prices charged for transactions that did not involve sanctioned entities.

38. It was further a part of the conspiracy that defendant MA oversaw and directed financial transactions conducted by defendant DHID that were intended to circumvent the prohibition against KKBC's use of the U.S. financial system. Defendant MA's signature was stamped on documents outlining the logistics of transactions guaranteed by KKBC that transacted through the U.S. in violation of IEEPA and the money laundering statutes.

39. It was further a part of the conspiracy that at no time relevant to this Indictment did any defendants apply for, receive, or possess a license or authorization from OFAC to engage in any transactions or dealings with a U.S. person or within the United States for the benefit of KKBC.

Overt Acts

40. In furtherance of the conspiracy, and to effect the illegal objects thereof, defendants DHID, MA, ZHOU, LUO, HONG, and their co-conspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about December 1, 2009, individuals affiliated with the North Korean government directed defendant ZHOU to forward an email to "CEO MA," with directions to reply back immediately, containing a U.S. dollar-denominated contract guaranteed by KKBC in which defendant DHID acted as a third party payer.

b. In or about December 2009, the KKBC branch office in Dandong contracted with defendant DHID to be a third-party payer on a \$6.85 million contract to purchase refined sugar using U.S. dollars for a North Korean company ("Company A"). Defendant DHID was identified on the contract as "the agent of the North Korean party."

c. In or about September 2009, defendants ZHOU and LUO coordinated U.S. dollar payments to a Singapore-based urea distributor ("Singapore Distributor") for the benefit of KKBC.

d. On December 9, 2009, a DHID front company made an approximately \$500,000 payment to the Singapore Distributor. The funds were transferred from a DHID front company account at China Merchants Bank in Shenzhen, China through China Merchants Bank's correspondent account at

Deutsche Bank AG and another U.S. correspondent account in the United States.

e. On or about December 6, 2011, defendant ZHOU emailed a China-based fertilizer distributor ("Chinese Distributor") about a contract for DHID's purchase of fertilizer. The contract was guaranteed by KKBC, and DHID had coordinated the purchase on behalf of another North Korean company ("Company B").

f. On January 16, 2012, a DHID front company paid the Chinese Distributor approximately \$1,014,163.90. The funds were transferred to the Chinese Distributor from the DHID front company's account at China Merchants Bank using China Merchants bank's correspondent account in the U.S.

g. On or about March 6, 2013, defendant ZHOU emailed a representative of Company B an offer by defendant DHID to sell Company B approximately 20,000 metric tons of fertilizer. Under the terms of the offer, DHID agreed to sell Company B approximately 20,000 tons of fertilizer packaged in 50 kilogram bags. The fertilizer was to be shipped from a port in China at the price of approximately \$480 per metric ton. The email further specified that the offer would be valid until on or about March 10, 2013. The offer also stated that before loading the cargo, defendant DHID first had to receive confirmation from KKBC that payment for the fertilizer had been deposited into a KKBC account by Company B.

h. From on or about May 6, 2013 through on or about June 21, 2013, DHID deposited approximately \$4,835,530 into a bank account at China

Merchants Bank held by one of its front companies registered in the British Virgin Islands. The approximately \$4,835,530 deposited in the front company's account was a payment to the Singapore Distributor. These funds were wired from China to the U.S. financial system using a U.S. correspondent bank account at Standard Chartered Bank and processed through Standard Chartered Bank's processing facility in Newark, New Jersey.

i. On or about January 3, 2014, defendant DHID sent Company B an offer to sell approximately 10,000 metric tons of fertilizer, conditioned on a thirty percent deposit from Company B and "a letter of credit from [KKBC] for the remaining 70% guaranteeing payment within 3 months from the [bill of lading] date."

j. On or about September 1, 2015, KKBC transferred approximately \$500,000 to a U.S. dollar account defendant DHID maintained at a North Korean branch of KKBC.

k. In or about 2013, in an email between defendant ZHOU and representatives from a Swiss company regarding a contract guaranteed by KKBC with a North Korea-based trading company, defendant ZHOU represented that defendant DHID and one of its front companies were "not owned or controlled or in any way linked to a sanctioned North Korean person/entity. . . ." Around the same time, defendant ZHOU also sent an email to the Swiss company, attaching a document that reported on KKBC's designation.

In violation of Title 18, United States Code, Section 371.

Count Two
(Conspiracy to Launder Monetary Instruments)

1. The allegations set forth in Paragraphs 1 through 27 and 29 through 40 of Count One of this Indictment are incorporated and re-alleged by reference herein.

2. From on or about December 9, 2009, through in or about September 2015, in Essex County, in the District of New Jersey and elsewhere, the defendants,

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT CO. LTD.,
MA XIAOHONG,
ZHOU JIANSHU,
HONG JINHUA, and
LUO CHUANXU,

and others did knowingly and intentionally conspire and agree with each other and others:

a. to transport, transmit, and transfer and attempt to transport, transmit, and transfer, monetary instruments and funds to a place in the United States from and through a place outside the United States, and from a place inside the United States to and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, a violation of IEEPA, contrary to Title 18, United States Code, Section 1956(a)(2)(A); and

b. to transport, transmit, and transfer and attempt to transport, transmit, and transfer, monetary instruments and funds to a place in the United States from and through a place outside the United States, and from a place inside the United States to and through a place outside the United States,

knowing that the monetary instrument or funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer was designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, that is, a violation of IEEPA, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i).

Objects of the Conspiracy

3. The objects of the conspiracy were:

a. To enrich the co-conspirators by conducting and promoting illegal business transactions with U.S. financial institutions using Chinese bank accounts established in the names of front companies to buy and sell commodities from foreign sellers and to make purchases using wire transfers to and from U.S. financial institutions;

b. To conceal and disguise the nature, location, source, ownership, and the control of the proceeds of the business transactions that were conducted in violation of U.S. laws and regulations.

In violation of Title 18, United States Code, Section 1956(h).

Count Three
(International Emergency Economic Powers Act)

1. The allegations set forth in Paragraphs 1 through 27 and 29 through 40 of Count One of this Indictment are incorporated and re-alleged by reference herein.

2. From in or about March 2013 to in or about June 2013, in Essex County, in the District of New Jersey, and elsewhere, the defendants,

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT CO. LTD.,
MA XIAOHONG,
ZHOU JIANSHU,
LUO CHUANXU, and
HONG JINHUA,

did knowingly and willfully violate and evade and avoid the restrictions imposed by the Office of Foreign Assets Control, U.S. Department of the Treasury, under the Weapons of Mass Destruction Proliferators Sanctions Regulations, Title 31, Code of Federal Regulations, Section 544.101, *et seq.*, by providing services on behalf of and for the benefit of a Specially Designated National, to wit, caused the provision of financial services and goods to and through the U.S. financial system for the benefit of and on behalf of Korea Kwangson Banking Corp., without first having obtained a license from the Office of Foreign Assets Control.

In violation of Title 50, United States Code, Section 1705(c), Title 31, Code of Federal Regulations, Sections 544.201 and 544.205, and Title 18, United States Code, Section 2.

Forfeiture Allegation as to Counts One And Three

1. The allegations set forth in Paragraphs 1 through 27 and 29 through 40 of Count One and Paragraph 2 of Count Three of this Indictment are incorporated and re-alleged by reference herein.

2. The United States hereby gives notice to the defendants,

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT CO. LTD.,
MA XIAOHONG,
ZHOU JIANSHU,
LUO CHUANXU, and HONG JINHUA,

that, upon conviction of the offenses charged in Counts One and Three of this Indictment, the government will seek forfeiture, in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of Title 50, United States Code, Section 1705(c), and Title 18 United States Code, Section 371. The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

Forfeiture Allegation as to Count Two

1. The allegations set forth in Paragraphs 2 and 3 of Count One and Paragraph 2 of Count Two of this Indictment are incorporated and re-alleged by reference herein.

2. The United States hereby gives notice to the defendants,

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT CO. LTD.,
MA XIAOHONG,
ZHOU JIANSHU,
LUO CHUANXU, and
HONG JINHUA,

that, upon conviction of the offense charged in Count Two of this Indictment, the government will seek forfeiture, in accordance with Title 18, United States Code, Section 982(a)(1), of any property, real or personal, involved in the offense in violation of Title 18, United States Code, Sections 1956, or any property traceable to such property. The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property, real or personal, involved in this offense, or any property traceable to such property.

Substitute Assets Provision

3. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendants:

- a. Cannot be located upon the exercise of due diligence;
- b. Has been transferred or sold to, or deposited with, a third party;
- c. Has been placed beyond the jurisdiction of the Court;
- d. Has been substantially diminished in value; or

- e. Has been commingled with other property that cannot be divided without difficulty;

It is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

A TRUE BILL

FOREPERSON

Craig Carpenito
CRAIG CARPENITO
United States Attorney

Deborah L. Connor (f.u.w.)
DEBORAH L. CONNOR
Chief, Money Laundering & Asset Recovery Section
Criminal Division, U.S. Department of Justice

Jay I. Bratt (af)
JAY I. BRATT
Chief, Counterintelligence and Export Control Section
National Security Division, U.S. Department of Justice

CASE NUMBER: _____

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

DANDONG HONGXIANG INDUSTRIAL DEVELOPMENT
CO. LTD, MA XIAOHONG, ZHOU JIANSHU, LUO CHUANXU, and HONG JINHUA

INDICTMENT FOR

18 U.S.C. §§ 371, 1956(h), 2 and 50 U.S.C. § 1705(c)

A True Bill, 1

Foreperson

CRAIG CARPENITO
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY

DEBORAH L. CONNOR
CHIEF, MONEY LAUNDERING & ASSET RECOVERY SECTION
CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

JAY I. BRATT
CHIEF, COUNTERINTELLIGENCE AND EXPORT CONTROL SECTION
NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

JOYCE M. MALLIET
ASSISTANT U.S. ATTORNEY
NEWARK, NEW JERSEY
973-645-2876

CHRISTIAN FORD
JENNIFER WALLIS
TRIAL ATTORNEYS, DEPARTMENT OF JUSTICE
